Alma Mater Studiorum – Università di Bologna

DOTTORATO DI RICERCA IN

DIRITTO E NUOVE TECNOLOGIE

curriculum "Informatica giuridica e diritto dell'informatica"

Ciclo XXVI

Settore Concorsuale di afferenza: 12/H3

Settore Scientifico disciplinare: IUS/20

Il Fascicolo Sanitario Elettronico tra Semantic Web e diritto alla privacy

Presentata da: Maria Gabriella Virone

Coordinatore Dottorato	**Relatore**
Prof. Giovanni Sartor	Prof.ssa Monica Palmirani

Esame finale anno 2014

"Credete nei vostri sogni: anche se a volte sembrano impossibili non buttateli, ma lottate per realizzarli. Più sono importanti, più il percorso che vi aspetta è difficile, ma vale la pena andare avanti, sempre. Solo così la vita diventerà la vostra vita"

(da C. PERROTTI, F. PASINETTI, *Lo sguardo oltre le dune*, Corbaccio, Milano, 2011)

INDICE

ABBREVIAZIONI

AA	Attribute Authority
APIs	Application Programming Interface
ATNA	Audit Trail and Note Authentication
BPPC	Basic Patient Privacy Consent
CDA	Clinical Document Architecture
CDR	Clinical Data Repository
CEN	European Committe for Standardization
CMR	Computerised Medical Record
Continua	Continua Health Alliance
CSE	Carta Sanità Elettronica
CT	Consistent Time
DICOM	Digital Imaging and Communications in Medicine
DMR	Digital Medical Record
ebXML	Electronic Business using eXtensible Markup Language
ECR	Electronic Client Record
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange For Administration, Commerce and Transport
EHR	Electronic Health Record
EMR	Electronic Medical Record
EPR	Electronic Patient Record
epSOS	Smart Open Services for European Patients
epSOS MTC	epSOS Master Translation/Transcoding
FSE	Fascicolo Sanitario Elettronico
FP7	Seventh EU Research Framework Programme
GP	General Practicer
HL7	Health Level 7
HPI	Healthcare Provider Index
HTTP	Hypertext Transfer Protocol
IBSE	Infrastruttura di Base per la Sanità Elettronica
IBIS	InfoBroker Individuale Sanitario

ICD	International Classification of Diseases
ICT	Information and Communication Technologies
IdP	Identity Provider
IEEE	Institute of Electrical and Electronics Engineers
IHE	Integrating the Healthcare Enterprise
IHTSDO	International Health Terminology Standards Development
InFSE	Infrastruttura Tecnologica del Fascicolo Sanitario Elettronico
IPSE	sperimentazione di un sistema per l'Interoperabilità europea e nazionale delle soluzioni di fascicolo sanitario elettronico: componenti Patient Summary ed Eprescription
ipSEC	Internet Protocol Security
ISO	International Organization for Standardization
LOD	Linked Open Data
LOINC®	Logical Observation Identifiers Names and Codes
LPI	Local Patient Index
MMG	Medico di Medicina Generale
NCP	National Contact Point
NEMA	National Electrical Manufacturers Association
NSIS	Nuovo Sistema Informativo Sanitario
OASIS	Organization for the Advancement of Structured Information Standards
OD	Open Data
OIO-XML	Offentlig Information Online eXtensible Markup Language
OMS	Organizzazione Mondiale alla Sanità
ONG	Organizzazione Non Governativa
PA	Profile Authority
PAP	Policy Administration Point
PbD	Privacy by Design
PCC	Patient Care Coordination
PDQ	Patient Demography Query
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PET	Privacy Enhancing Technology
PHR	Personal Health Record

PHR	Population Health Record
PIP	Policy Information Point
PIX	Patient Identifier Cross Referencing
PSE	Piano di Sanità Elettronica
P3P	Platform for Privacy Preferences
RBAC	Role-Based Access Control
RBAC	Rule-Based Access Control
RDF	Resource Description Framework
Rel	Release
RIM	Reference Information Model
SAML	Security Assertion Markup Language
SNOMED CT	Systematized Nomenclature of Medicine - Clinical Terms
SPARQL	SPARQL Protocol and RDF Query Language
SPCoop	Sistema Pubblico di Connettività e Cooperazione
STS	Security Token Service
TIC	Tecnologie dell'Informazione e della Comunicazione
TC	Technical Commission
TL/SSL	Trasport Layer Security
UE	Unione europea
URI	Uniform Resource Identifier
VPN	Virtual Private Network
WHO	World Health Organization
WS-Security	Web Services Security
WS-Trust	Web Services Trust
XACML	eXtensible Access Control Markup Language
XCA	Cross Community Assertion
XDS	Cross Enterprise Document Sharing
XML	eXtensible Markup Language
XUA	Cross Enterprise User Assertion
W3C	World Wide Web Consortium

INDICE DELLE FIGURE

INTRODUZIONE

SOMMARIO: 1. Il contesto - 2. Gli obiettivi della ricerca - 3. La metodologia - 4. La struttura

1. IL CONTESTO

L'applicazione delle Tecnologie dell'Informazione e della Comunicazione (TIC) nei sistemi sanitari è oggi una realtà; conoscere le potenzialità dei nuovi strumenti è essenziale non soltanto per adottare soluzioni funzionali alla semplificazione ed al contenimento dei costi, ma, soprattutto, per valorizzare una partecipazione attiva e consapevole del "paziente digitale"[1].

Analogamente, il Fascicolo Sanitario Elettronico (FSE) è considerato in letteratura come un importante mezzo per il raggiungimento degli auspicati risultati di sanità digitale (supporto ai processi operativi, miglioramento della qualità dei servizi, riduzione della spesa pubblica), ma altrettanto fondamentale per l'assistenza, frontaliera e transfrontaliera, ai pazienti, nonché per il raggiungimento di un'effettiva e più ampia cooperazione tra le pubbliche amministrazioni coinvolte tanto a livello nazionale quanto a livello europeo. In questo senso, dunque, il Fascicolo Sanitario Elettronico non è mero spazio fisico per la registrazione di dati, sebbene questi ne costituiscano il nucleo vitale.

Principali dati contenuti nel FSE sono l'anagrafica per l'identificazione dell'utente nonché informazioni attinenti la storia clinica dell'assistito (ricoveri ospedalieri, specialistica ambulatoriale, prestazioni farmaceutiche, assistenza residenziale, assistenza domiciliare, accessi al Pronto Soccorso etc.).

Con specifico riferimento ai processi diagnostico-terapeutici, funzioni paradigmatiche del FSE sono: (i) registrare con precisione e rendere rapidamente reperibili i dati sulle indagini in programma e sui trattamenti prescritti ed effettivamente somministrati; (ii) fornire l'interpretazione dei dati avanzata dal medico responsabile del paziente nonché i motivi che hanno indotto ad iniziare, sospendere o modificare un trattamento ovvero propendere per l'esecuzione di un esame di laboratorio o di un'indagine strumentale; (iii) consentire una comunicazione efficiente e rapida fra i diversi operatori sanitari per una gestione condivisa dei problemi dell'assistito; (iv) rendere espliciti e giustificare i motivi razionali

[1] Con tale accezione ivi s'intende sottolineare il mutamento di approccio, rispetto ad una visione tradizionale, dell'assistito con il Sistema Sanitario, per quanto concerne le modalità di accesso e fruizione dei servizi di assistenza, i processi di prevenzione e cura, così come, sempre più frequentemente, le dinamiche relazionali con il personale sanitario (medico di medicina generale/pediatra di libera scelta o specialista).

delle decisioni terapeutiche in caso di contestazioni in sede medico-legale.

Oggetto di crescente interesse, tanto da parte dell'Unione europea e dei 27 Paesi membri quanto dei pazienti stessi, il Fascicolo Sanitario Elettronico può, quindi, contribuire ad una miglior cura del paziente nonché agevolare un accesso semplice ed efficace ai servizi sanitari. In questo scenario, tanto la Pubblica Amministrazione quanto l'utente sono attori privilegiati, verso cui, peraltro, *standard*[2] tecnici, politiche comunitarie, norme e prassi vigenti sono chiamate ad orientarsi, soprattutto, a fronte dei livelli, elevati e stabili, di mobilità che richiedono rapide forme di accessibilità e scambio delle informazioni sanitarie. Per raggiungere tali obiettivi, gli Stati membri dell'Unione europea, con l'Agenda digitale europea, si sono, ad esempio, impegnati ad intraprendere due azioni (13 e 14): (i) dotare i cittadini europei di un accesso *online* sicuro ai dati sanitari entro il 2015; (ii) definire *standard* per l'interoperabilità europea dei Fascicoli Sanitari Elettronici.

Il quadro sinteticamente illustrato risente, però, di significativi ostacoli attuativi, di tipo culturale, tecnologico e giuridico. Società multietnica in cui convivono lingue e tradizioni (anche mediche) plurime, *digital divide*, banda larga non uniforme sul territorio nazionale, regole tecniche spesso frammentate, sistemi informativi frequentemente non interconnessi, normativa internazionale, europea e nazionale eterogenea, limitata cooperazione transfrontaliera tra le pubbliche amministrazioni sono, infatti, soltanto alcune tra le criticità che richiedono maggiore attenzione da parte di politici ed esperti di settore.

Non è di secondaria importanza, altresì, evidenziare la logica con cui dati e documenti sanitari digitali sono, spesso, a tutt'oggi, strutturati: essa, infatti, come segnalano esperti ed operatori del settore, così come emerge dai documenti tecnici di settore, è ancora fortemente incentrata sulle già consolidate versioni cartacee. In altri termini, in numerosi casi, la struttura dei dati medici si presenta come mera trasposizione degli analoghi documenti di tipo analogico, compromettendo, di conseguenza, la semantica e l'interoperabilità delle informazioni.

Ciò spiega le ragioni per cui lavorare sul concetto di interoperabilità è una pista strategica sia nazionale (centrale e locale) sia comunitaria. Operare a tale livello richiede, tuttavia, una forte sinergia per la predisposizione di modelli architetturali di FSE che rispettino da una parte gli *standard* sintattici, semantici, tecnici ed organizzativi, la cui necessità più volte è stata ribadita dalla Commissione europea, dall'altra le discipline vigenti e le prassi in essere in materia di protezione dei dati personali, considerata la natura sensibile delle

[2] Nel rispetto delle più severe regole della linguistica generale, nel presente lavoro la forma plurale dei forestierismi non adattati non è stato utilizzata.

informazioni raccolte nel Fascicolo Sanitario Elettronico.

La *figura 1*, di seguito riportata, tratteggia il contesto presentato, a partire dal quale è stato articolato il presente studio.

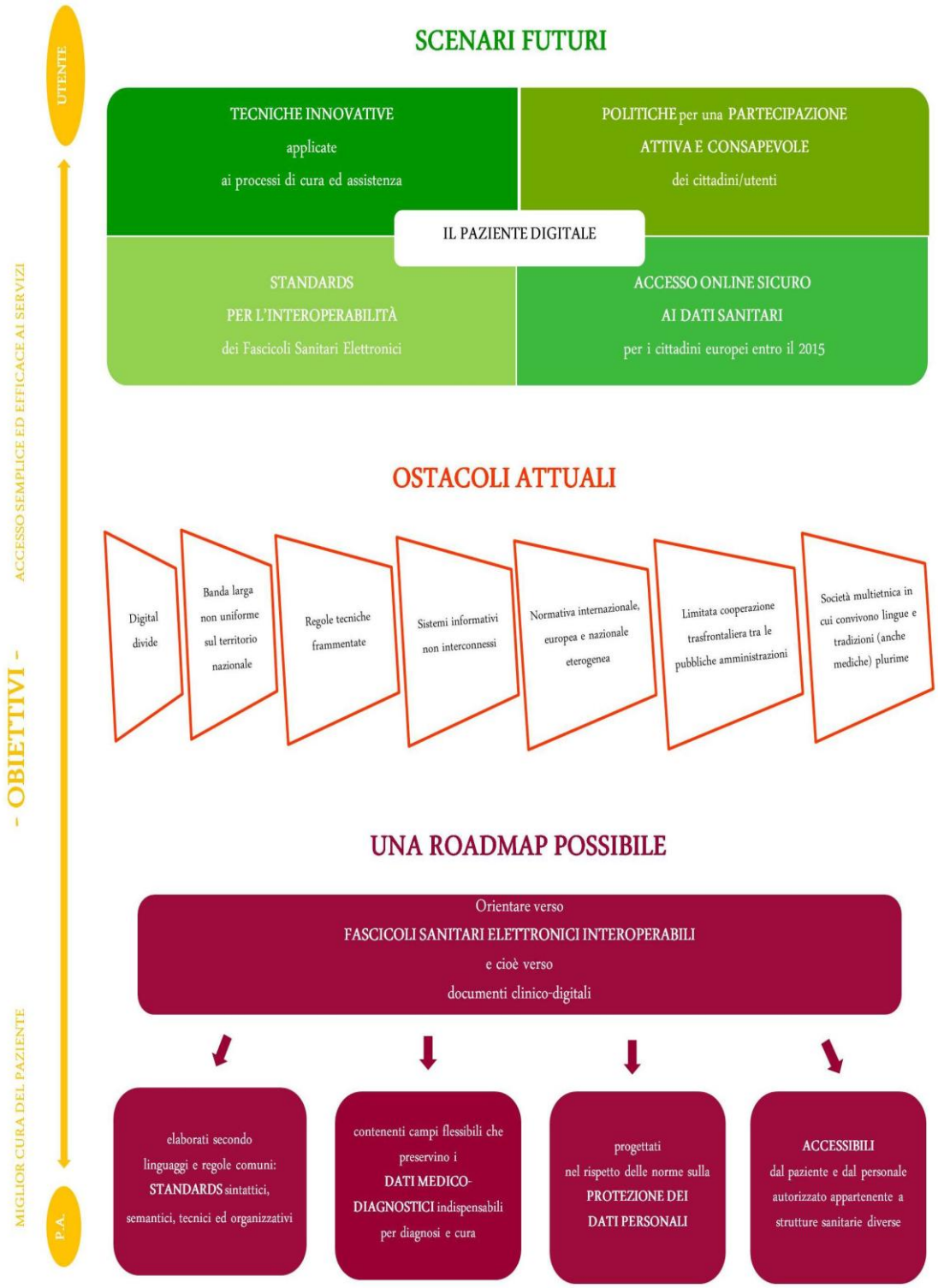


Figura 1 - Il Fascicolo Sanitario Elettronico tra *Semantic Web* e diritto alla *privacy*[3]

[3] La figua 1 è stata presentata da Maria Gabriella Virone come "Poster" durante l'iniziativa "Progetti in mostra" (Bologna, 17-25 maggio 2012), organizzata da Università di Bologna e Fondazione Alma Mater, cui

2. GLI OBIETTIVI DELLA RICERCA

Obiettivo generale della ricerca è stato quello di ricostruire, in modo sistematico ma funzionale, lo stato dell'arte in materia di Fascicolo Sanitario Elettronico, con una precipua attenzione ai temi della protezione dei dati personali e degli *standard* in sanità nonchè alle "relazioni" tra questioni giuridiche e tecnologiche.

Obiettivi specifici della ricerca sono stati, anzitutto, quello di delineare le criticità esistenti nello stato dell'arte e di suggerire nuovi approcci soprattutto in merito all'utilizzo con finalità secondarie dei dati collezionati nel FSE. Tale profilo implica la necessità di nuove riflessioni tecnico-giuridiche, sia per ciò che concerne il *design* dei sistemi informativi sia per ciò che concerne visioni di garantismo *a priori* relative all'utilizzo dei dati sanitari.

3. LA METODOLOGIA

Le peculiarità del *curriculum* "Informatica giuridica e diritto dell'informatica" del dottorato di ricerca in "Diritto e nuove tecnologie" hanno orientato verso una lettura tecnico-giuridica delle problematiche inerenti il Fascicolo Sanitario Elettronico.

Si è preferita una prospettiva critica che, senza eludere il dettaglio di alcuni profili essenziali per la comprensione dello strumento esaminato, ha, però, voluto favorire un approccio per "questioni aperte".

L'attenzione al più ampio tema della sanità digitale, nel quale il FSE si colloca, è stata inevitabile, così come inevitabile è stata la contestualizzazione europea del tema in esame. L'analisi delle strategie politiche, delle norme vigenti, delle azioni in essere ha permesso di delineare lo scenario comunitario nel quale l'*e-Health* assume un ruolo di grande interesse.

La revisione della letteratura esistente ha, poi, consentito di definire le peculiarità architetturali del FSE e le relative potenzialità. In particolare, attraverso lo studio di selezionati progetti sono stati individuati gli *standard* utilizzati nei sistemi informativi di FSE; ciò ha permesso di individuare le principali affinità tecnologiche e, parimenti, di osservare le criticità soprattutto legate alla struttura dei dati.

Per ciò che concerne la parte normativa della ricerca, in particolare le questioni in materia di protezione dei dati personali e la definizione di un contesto nazionale dedicato al FSE, in un certo senso può asserirsi che l'opera non è conclusa. Dal gennaio 2011, anno di

---

hanno partecipato i giovani ricercatori delle Scuole di dottorato dell'Alma Mater Studiorum – Università di Bologna. Il Poster "Il Fascicolo Sanitario Elettronico tra *Semantic Web* e diritto alla *privacy*" ha ricevuto l'attestato di merito "miglior poster per l'efficacia comunicativa all'interno dell'area umanistica".

inizio del presente lavoro, ad oggi, notevoli mutamenti sono in corso, sia sul fronte comunitario (pensiamo ad esempio alla "Proposta di regolamento sulla protezione dei dati personali" del 25 gennaio 2012), sia su quello nazionale (dall'assenza di disposizioni cogenti sul FSE, si è infatti arrivati ai recenti provvedimenti di rango primario sul FSE - decreti-legge 179/2012 e 69/2013 -, alcuni dei quali sono oggetto di discussione - trattasi dello "schema di decreto sul Fascicolo Sanitario Elettronico" attualmente all'esame della Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e Bolzano -).

I principi in tema di "*Privacy by Design*" e di "*Open Data*" hanno sollecitato nuove considerazioni rispetto all'assetto originale della presente ricerca. In particolare, un ruolo fondamentale è stato riconosciuto al dato sanitario de-identificato collezionato nel FSE nonché alla valenza di tale informazione per finalità secondarie, di sanità pubblica e ricerca. Da qui, la convinzione di una lettura sinergica e, forse nuova, dei concetti di *security* e *privacy* nella modellazione di sistemi informativi sanitari nonché l'importanza di sostenere modelli di armonizzazione tecnico-giuridici.

4. LA STRUTTURA

Lo studio si articola in *quattro capitoli* che hanno lo scopo di tratteggiare lo stato dell'arte in materia di Fascicolo Sanitario Elettronico. L'attenzione al contesto europeo nel quale la storia di questo strumento di sanità elettronica si colloca è stata, però, imprescindibile: politiche, norme, tecnologie e prassi di interesse hanno, infatti, anticipato le azioni italiane in essere, a cui è stata inevitabilmente dedicata buona parte della ricerca.

Il *capitolo I*, intitolato "*e-Health* e Fascicolo Sanitario Elettronico. Prospettive politiche e giuridiche dell'Unione europea", ripercorre le tappe principali in materia di sanità elettronica, fin dai primi impulsi all'*e-Health* nei piani dell'Unione europea. *Leitmotiv* della ricerca è stato il concetto di interoperabilità dei sistemi informativi sanitari, ribadita da precisi provvedimenti comunitari di cui si è dato riscontro. Sono stati, infine, richiamati i più recenti provvedimenti europei sull'*e-Health*, quali, ad esempio, "Europa 2020" ed il "Piano d'azione Sanità Elettronica 2012-2020" da cui emergono priorità e strategie per il futuro a cui sono chiamati ad orientarsi i 27 Paesi membri.

Il *capitolo II*, dedicato a "Il Fascicolo Sanitario Elettronico nell'attuale scenario europeo ed italiano", ha una connotazione prevalentemente tecnica. Definito il concetto di FSE, alla luce della letteratura esistente in materia, lo studio considera per brevi cenni il processo di standardizzazione in sanità, ricordando le principali organizzazioni di standardizzazione.

Tale introduzione è funzionale all'analisi di selezionati progetti, europei e nazionali, che ha avuto ad oggetto gli elementi essenziali dell'architettura del FSE. In particolare, esaminati i progetti in essere tra i 27 Stati membri, tenuto conto di esperienze pilota europee, di contesti con avanzate e solide radici nel settore dell'*e-Health*, di azioni di più recente evoluzione sia tecnica sia giuridica sul FSE nonché dello scenario italiano, lo studio ha riferito, per precise ragioni, dei seguenti prodotti: progetto "*Smart Open Services for European Patients*" (UE); progetto "*ELGA - Elektronische Gesundheitsakte*" (Austria); progetto "*MedCom*" (Danimarca); progetto "*Infrastruttura tecnologica del Fascicolo Sanitario Elettronico*", progetto "*OpenInFSE: Realizzazione di un'infrastruttura operativa a supporto dell'interoperabilità delle soluzioni territoriali di fascicolo sanitario elettronico nel contesto del sistema pubblico di connettività*", progetto "*Evoluzione e interoperabilità tecnologica del Fascicolo Sanitario Elettronico*", progetto "*IPSE - Sperimentazione di un sistema per l'interoperabilità europea e nazionale delle soluzioni di Fascicolo Sanitario Elettronico: componenti Patient Summary e ePrescription*" (Italia).

Il *capitolo III* affronta la questione dei "Sistemi informativi e dati personali in sanità elettronica", a partire da una lettura, il più possibile armonica, dei temi tecnici e giuridici. Sicurezza dei sistemi informativi sanitari e protezione dei dati personali sono, infatti, aspetti distinti ma complementari, dal momento che la loro implementazione salvaguardia un interesse inerente ora una persona fisica ora un sistema. Individuati i profili di sicurezza dei sistemi informativi, la ricerca considera i principi giuridici, comunitari e nazionali, sul trattamento dei dati personali e sanitari, fino alla più recente normativa in materia di sanità digitale e Fascicolo Sanitario Elettronico.

Il *capitolo IV* intende cogliere "La sfida tecnologica: sicurezza e riuso dei dati sanitari", accogliendo l'idea di considerare i dati de-identificati raccolti nel FSE come risorsa per le sfide sociali e fonte per la conoscenza scientifica. Nel rigoroso rispetto delle norme in tema di trattamento dei dati personali, è possibile aprire un'importante riflessione sull'applicabilità dei principi di "*Open Data*" e "*Linked Open Data*" anche al FSE, quale concreta risposta all'esigenza di interoperabilità. L'auspicio è, dunque, l'armonizzazione dei profili tecnologico e legislativo a beneficio della tutela del diritto alla salute, anche a partire dall'implementazione della "*Privacy by Design*".

CAPITOLO I

E-HEALTH E FASCICOLO SANITARIO ELETTRONICO. PROSPETTIVE POLITICHE E GIURIDICHE DELL'UNIONE EUROPEA

SOMMARIO: 1. La "sanità elettronica" - 2. I primi impulsi all'*e-Health* nei piani dell'Unione europea - 3. Verso una società dell'informazione *sicura* ed *interoperabile* - 4. "Europa 2020": priorità e strategie europee per l'*e-Health* - 5. Le strategie nazionali degli Stati membri - 6. Una sanità innovativa per il 21esimo secolo: il "Piano d'azione Sanità Elettronica 2012-2020"

1. LA "SANITÀ ELETTRONICA"

Per sanità elettronica o *e-Health* s'intende in generale l'utilizzo delle nuove tecnologie nel dominio sanitario allo scopo di migliorare l'accesso degli utenti all'assistenza medica[4], la sicurezza dei pazienti grazie alla riduzione del rischio clinico[5], la qualità e l'efficacia delle prestazioni erogate dai servizi sanitari nazionali nonché la stessa produttività dei sistemi, contenendo sprechi e diseconomie frequentemente dovuti a ricorsi impropri da parte degli assistiti e ad una errata gestione dei profili organizzativi ed amministrativi[6].

Aspetti centrali del concetto di *e-Health* sono da una parte quello di salute, definita dall'Organizzazione Mondiale alla Sanità (OMS) come "stato di completo benessere fisico, psichico, sociale e non soltanto come assenza di malattia"[7], dall'altra quello di digitale, inteso come uso delle tecnologie applicate agli strumenti diagnostici, ai processi

[4] Tesi sostenuta in N. WALLERSTEIN, *What is the evidence on effectiveness of empowerment to improve health?*, WHO Regional Office for Europe, Health Evidence Network report, Copenhagen, 2006.

[5] Concordano su questo profilo: M. ABDELHAK, *Health Information Management of a Strategic Resource*, W.B. Saunders Company, Philadelphia, PA, 1996; D.W. BATES, J.M. TEICH, J. LEE, D. SEGER, G.J. KUPERMAN, N. ET AL MA'LUF, *The impact of computerized physician order entry on medication error prevention*, Journal of the American Medical Informatics Association", 6(4), 1999, pp. 313-321; D.S. CANNON, S.N. ALLEN, *A comparison of the effects of computer and manual reminders on compliance with a mental health clinical practice guideline*, Journal of American Medical Information Association, 7, 2000, pp.196-203.

[6] Secondo quanto affermato in P.M. DANZON, M. FURUKAWA, *e-Health: Effects of the Internet on Competition and Productivity in Health Care*, The Economic Payoff from the Internet Revolution, the Brookings Task Force on the Internet, Brookings Institution Press: Washington, 2001.

[7] Definizione contenuta nel Preambolo della *Constitution of the World Health Organization* (1946 - Official Records of the World Health Organization 2, 100), amended WHA 26.37, WHA 29.38, WHA 39.6 and WHA 51.23, WHO Basic documents Forty-fifth edition, Supplement, October 2006.

organizzativi dei sistemi sanitari, al mercato etc.

Diritto fondamentale della persona ed ottimizzazione dei servizi coesistono, dunque, in questo settore in costante evoluzione. Tuttavia, i due profili indicati (diritto e tecnologia) non sempre sono egualmente considerati come parti essenziali, coesistenti e complementari, della medesima realtà: in taluni casi, infatti, sono maggiormente accentuate le connotazioni tecniche e di gestione, in altri casi le questioni giuridiche. É, invece, importante pensare alla sanità elettronica come ad un tessuto fitto di trame tra loro intrecciate ed interdipendenti, caratterizzato, tra l'altro, da forti rapporti negoziali, esistenti tra tutti gli *stakeholder* coinvolti nei processi sanitari, quali Governi, sistemi sanitari nazionali e loro operatori, pazienti/utenti e loro famiglie, compagnie assicurative, aziende impegnate sul fronte biomedico, enti di ricerca e di innovazione. Tutti i soggetti summenzionati sono, quindi, costantemente tenuti a mantenere un dialogo vivo e propositivo, al fine di contribuire all'adozione di prassi, giuridiche e tecniche, effettivamente bilanciate e migliorative della cura della persona.

Risponde a questa logica la definizione, ormai decennale, ma sempre attuale proprio per la sua multidisciplinarietà, proposta da Eysenbach, secondo cui: *"e-Health is an emerging field in the intersection of medical informatics, public health and business, referring to health services and information delivered or enhanced through the Internet and related technologies. In a broader sense, the term characterizes not only a technical development, but also a state-of-mind, a way of thinking, an attitude, and a commitment for networked, global thinking, to improve health care locally, regionally, and worldwide by using information and communication technology"*[8].

L'*e-Health* è, dunque, un macro-fenomeno descrivibile secondo i modelli rappresentativi dei mercati, nei quali, soggetti e processi coinvolti sono elevati, sia per numero sia per complessità[9]. In particolare, oltre alle figure primariamente implicate nelle

[8] G. EYSENBACH, *What is e-health?*, Journal of Medical Internet Research 3(2):e20, 2001. Nel delineare il concetto di *e-health* l'Autore ha individuato dieci caratteristiche ad esso strettamente collegate: *efficiency, enhancing quality, evidence based, empowerment - of consumers and patients - by making the knowledge bases of medicine and personal electronic records accessible to consumers over the Internet, e-health opens new avenues for patient-centered medicine, and enables evidence-based patient choice; encouragement, education, enabling information exchange and communication in a standardized way between health care establishments; extending the scope of health care beyond its conventional boundaries, ethics, equity*.
Nella presente ricerca non si darà conto delle numerose definizioni di *e-Health* rintracciabili in letteratura; per approfondimenti si rinvia a H. OH, C. RIZO, M. ENKIN, A. JADAD, *What Is eHealth (3): A Systematic Review of Published Definitions*, Journal of Medical Internet Research, Jan-Mar; 7(1): e1, 2005.

[9] Per approfondimenti: L. VALERI, D. GIESEN, P. JANSEN, K. KLOKGIETERS, *Business Models for eHealth. Final Report. Prepared for ICT for Health Unit DG Information Society and Media European Commission*, 2010, pp.75; EUROPEAN COMMISSION - INFORMATION SOCIETY AND MEDIA DIRECTORATE-GENERAL, *eHealth Benchmarking III. SMART 2009/0022. Final Report*, Deloitte&Ipsos Belgium, 2011, pp. 274.

dinamiche di erogazione e fruizione delle prestazioni sanitarie (personale sanitario, parasanitario ed amministrativo da una parte, e cittadini/pazienti dall'altra), sono altresì presenti i *policy maker* responsabili della sanità pubblica (come ad esempio i Governi) nonché tutti i soggetti, pubblici e privati, persone fisiche e giuridiche, interessati alla vendita ed all'acquisto di beni e servizi funzionali alle attività connesse all'introduzione delle nuove tecnologie nel settore sanitario (tra cui *partner* commerciali, aziende ed enti di ricerca pubblici e privati etc.).

Come emerge dall'indagine conoscitiva realizzata nel 2006 da "*Global Observatory for e-Health*"[10] dell'Organizzazione Mondiale alla Sanità (OMS), la sanità elettronica rappresenta un'area in progressiva crescita, nella quale i soggetti coinvolti costantemente necessitano di validi mezzi ed adeguati servizi. Particolarmente interessante ai fini della presente ricerca è notare che, in questo primo studio condotto a livello globale, i fascicoli sanitari elettronici furono individuati tra gli strumenti da sviluppare nei contesti nazionali e che l'OMS auspicò la creazione di una risorsa digitale a beneficio degli Stati membri dedicata ai temi delle strategie e delle *policy* in materia di *e-Health* nonché ai profili della sicurezza e delle questioni giuridiche rilevanti per il dominio in esame. Tali dati confermano l'importanza di agire secondo strategie ed azioni coordinate tra gli Stati, conclusione questa che trova una plausibile spiegazione nel fatto che la salute è, congiuntamente, diritto fondamentale dell'individuo ed interesse della collettività[11].

In questo scenario è palese che gli interessi in gioco sono cospicui e tra loro talora discordanti, al punto da richiedere mirati interventi politico-legislativi a livello nazionale e sovranazionale. Il diritto di accesso alle cure ed alla protezione dei dati personali dei pazienti, la responsabilità medica, la correttezza nelle transazioni commerciali, sono solo alcuni dei tanti aspetti oggetto di specifiche disposizioni e normative europee, che, tuttavia, in taluni casi, richiedono puntuali revisioni, dovute non da ultimo al fatto che i concetti e gli istituti giuridici non seguono lo stesso progressivo e rapido mutamento delle nuove tecnologie.

La digitalizzazione del settore sanitario non è un fenomeno di recente diffusione né se si considera l'uso delle Tecnologie dell'Informazione e della Comunicazione nelle applicazioni medico-diagnostiche né se si prende in rassegna l'impegno politico e giuridico comunitario e nazionale. Intorno agli anni Sessanta, fisici, matematici e medici iniziano ad

[10] WORLD HEALTH ORGANIZATION, *eHealth. TOOLS&SERVICES. Needs of the Member States. Report of the WHO Global Observatory for eHealth*, Switzerland, WHO/EHL/06.1, 2006, pp. 30.
[11] Secondo quanto sancito dal primo comma dell'articolo 32 della Costituzione italiana.

occuparsi di sanità elettronica, prestando speciale attenzione ai profili biomedici[12]. Se, poi, si esaminano le strategie d'azione promosse dall'Unione europea ed i conseguenti piani operativi posti in essere dai 27 Paesi membri, dalla fine degli anni Novanta e, con maggiore continuità dagli inizi del Nuovo Secolo, molteplici sono stati i documenti, cogenti e non, adottati a livello comunitario che hanno avuto ad oggetto l'*e-Health* nelle sue diverse concretizzazioni.

La razionalizzazione della spesa sanitaria pubblica, l'organizzazione di strutture e di sistemi fortemente complessi, la collaborazione tra i professionisti sanitari mediante strumenti di telemedicina, l'accesso alle informazioni sull'assistenza ed alle cure da parte degli utenti, l'aggregazione e l'immediata disponibilità di dati anagrafici e clinici in cartelle sanitarie digitali, sono solo alcuni tra i tanti profili esaminati dalla Commissione europea, la quale rivolge una considerevole attenzione anche ai crescenti ed attuali fenomeni della mobilità internazionale, del multiculturalismo e del plurilinguismo che, sempre più, caratterizzano la società contemporanea ed i cui risvolti, peraltro, nella tematica dell'assistenza sanitaria, sono di significativa rilevanza.

Gli Organi comunitari mostrano, inoltre, particolare interesse verso questioni quali il trattamento e la protezione dei dati personali, l'adozione di idonee misure di sicurezza, l'utilizzo di *standard*, l'interoperabilità fra i diversi sistemi, aspetti questi che verranno considerati in dettaglio nel corso del presente lavoro.

L'attenzione politica e le implicazioni legislative delle proposte sorte attorno al tema delineato sono, altresì, corroborate dall'erogazione di molteplici finanziamenti, attraverso i quali, nell'ultimo ventennio, l'Unione europea ha favorito la realizzazione di progetti ed iniziative, nazionali ed internazionali, volti a sviluppare ed implementare un vero e proprio spazio europeo per la sanità elettronica. I settori di intervento sono alquanto vari, sia per la natura poliedrica del dominio sanitario sia per le continue evoluzioni che caratterizzano le nuove tecnologie[13].

Quanto premesso introduce all'analisi dei documenti europei a partire dai quali l'*e-Health* ha avuto impulso nonché di quelli più recenti che orientano verso nuovi possibili

[12] Interessante in proposito E.H. SHORTLIFFE, M.S. BLOIS, *The computer meets medicine and biology:emergence of a discipline*, in E.H. Shortliffe, L.E. Perrault, G. Widerhold, L.M. Fagan (eds.), *Medical informatics: computer applications in health care and biomedicine*, 2nd ed., New York, Springer, 2001:3-40.

[13] A confermare l'attualità e l'interesse che la sanità elettronica e, più in generale, la digitalizzazione destano a livello comunitario e, quindi, l'importanza di perseguire azioni espressamente dedicate a tali tematiche, sono, tra gli altri, l'ultimo programma di finanziamenti europei per la ricerca "*Horizon 2020*" ed il "Programma per la competitività delle imprese e le PMI (COSME) 2014-2020", i cui risultati saranno però valutabili soltanto nei prossimi anni.

futuri scenari (*cfr. fig. 2*).

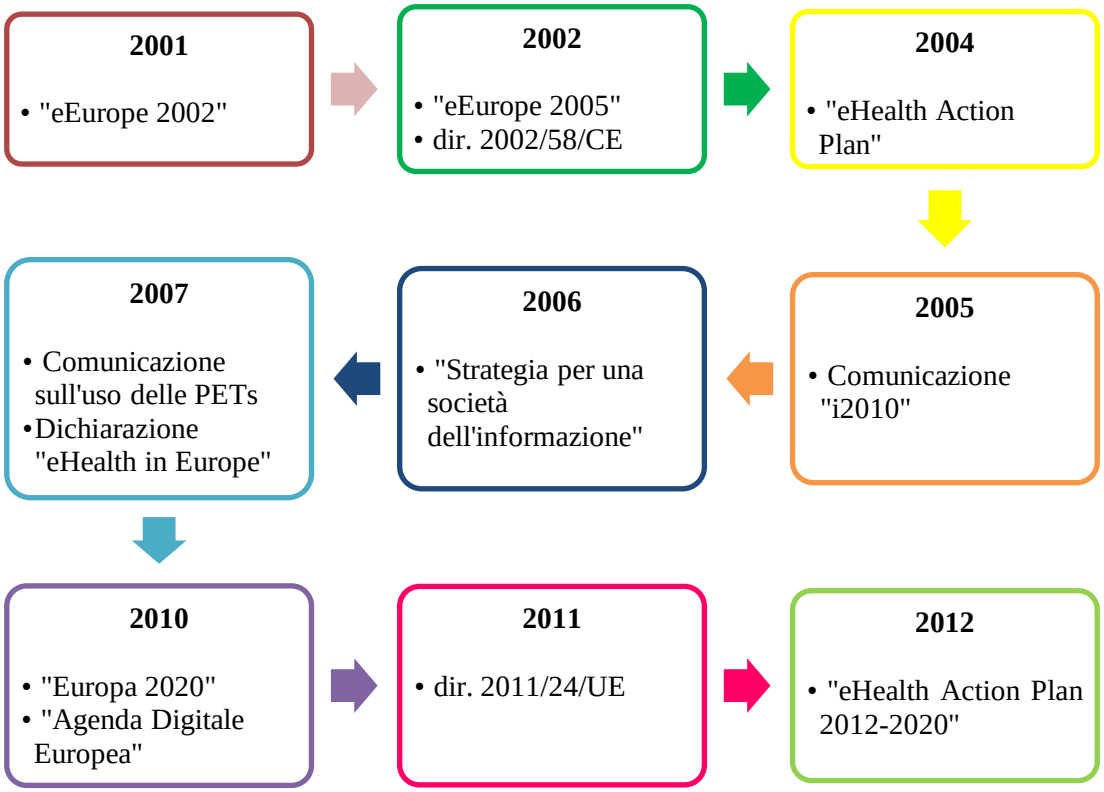


Figura 2 - Selezionati documenti europei in materia di *e-Health*

2. I PRIMI IMPULSI ALL'*E-HEALTH* NEI PIANI DELL'UNIONE EUROPEA

Facendo seguito al piano d'azione "*eEurope 2002*"[14], volto ad accelerare la società dell'informazione in Europa e la disponibilità della stessa per tutti, nel giugno 2002, in vista del Consiglio europeo di Siviglia, la Commissione redasse la Comunicazione "eEurope 2005: una società dell'informazione per tutti"[15] il cui principale obiettivo fu stimolare la creazione di servizi, applicazioni e contenuti sicuri basati su una banda larga distribuita, in particolare nei settori di *e-government*, *e-learning*, *e-business* e *e-health*. Tre le proposte nel campo della sanità digitale da realizzare entro il 2005: predisporre e diffondere una Tessera Europea di Assicurazione della Malattia e consolidare

[14] COMMISSIONE DELLE COMUNITÀ EUROPEE, *Comunicazione della Commissione al Consiglio ed al Parlamento. eEurope 2002. Impatto e priorità. Comunicazione al Consiglio europeo di primavera, Stoccolma 23-24 marzo 2001*, Bruxelles, 13.3.2001, COM(2001) 140 definitivo.
[15] COMMISSIONE DELLE COMUNITÀ EUROPEE, *Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato Economico e Sociale e al Comitato delle Regioni, eEurope 2005: una società dell'informazione per tutti. Piano d'azione da presentare per il Consiglio europeo di Siviglia 21 e 22 giugno 2002*, Bruxelles, 28.5.2002, COM(2002) 263 definitivo.

un'architettura standardizzata per la creazione di fascicoli sanitari elettronici; promuovere l'utilizzo di *network* informativi sanitari; orientare verso l'erogazione di servizi di medicina *online* a beneficio dei cittadini. Parallelamente alle summenzionate azioni, per il raggiungimento dei risultati auspicati, si riconobbe l'importanza e, al contempo, la necessità, di aggiornare e migliorare le legislazioni, comunitaria e nazionali.

L'impulso verso la digitalizzazione dell'Unione spinse la Commissione a definire una Comunicazione, coeva alle precedenti, per sottolineare, con particolare intensità, il ruolo dell'*e-government* per il futuro dell'Europa: un coinvolgimento diretto e pro-attivo dei cittadini ed una visibile riorganizzazione aziendale possono contribuire al miglioramento dei servizi pubblici, in termini di efficacia ed efficienza; effetti immediati di tale concreta interazione sono, tra gli altri, la riduzione dei tempi di attesa ed il contenimento dei costi relativi all'erogazione delle prestazioni[16]. Il sistema sanitario, in quanto servizio pubblico, è collocato nel medesimo contesto; anch'esso non può, pertanto, essere esente da un processo di rinnovamento strutturale. In tal senso, essenziale diventa ripensare alle tradizionali forme organizzative e definire un impianto istituzionale *patient-based*, in cui l'interazione ed il dialogo tra la tecnologia e l'utente spingano verso un processo di semplificazione del complesso apparato burocratico[17]. Tra i risultati di un approccio così definito rientra, certamente, l'acquisizione di un buon livello di *empowerment* da parte dei pazienti[18], di cui, di fatto, beneficiano non soltanto l'individuo, ma anche i sistemi sanitari nonché la stessa società civile[19].

Le anzidette considerazioni non tardano a concretizzarsi in un altro documento ufficiale: nel luglio 2004, a seguito de "*e-Health 2005 Conference*", tenutasi a Tromso, la

---

[16] COMMISSIONE DELLE COMUNITÀ EUROPEE, *Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato Economico e Sociale e al Comitato delle Regioni*, *Il ruolo dell'eGovernment per il futuro dell'Europa*, Bruxelles, 26.9.2003, COM(2003) 567 definitivo.

[17] Si rinvia, tra gli altri, a J. ALLAN, J. ENGLEBRIGHT, *Patient-Centered Documentation: An Effective and Efficient Use of Clinical Information Systems*, Journal of Nursing Administration, 30(2):90-95, 2000.

[18] Di interesse sul tema: C. PAGLIARI, D. DETMER, P. SINGLETON, *Potential of electronic personal health records*, British Medical Journal, pp. 330-333, 2007; P. WILSON, C. LEITNER, A. MOUSSALLI, *Mapping the Potential of eHealth. Empowering the citizen through eHealth tools and services*, Maastricht, European Institute of Public Administration, 2004; C. TSAI, J. STARREN, *Patient Participation in Electronic Medical Records*, Journal of the American Medical Association, 285(13), 2001, p. 1765. Per altri contributi si rinvia a: M.A. ZIMMERMAN, *Empowerment Theory: Psychological, Organizational and Community Levels of Analysis*, in J. Rappaport, E. Seidman, "Handbook of Community Psychology", New York, Kluwer Academic/Plenum Publishers, 2000, pp. 43-63; G. LAVERACK, R. LABONTE, *A Planning Framework for Community Empowerment Goals within Health Promotion*, in "Health Policy and Planning", Vol. 15, n. 3, 2000, pp. 255-262; E.O. COX, R.J. PARSONS, *Empowerment oriented Social Work Practice with the Elderly*, Pacific Grove, Brooks/Cole Pub. Co., 1994.

[19] Tali concetti sono stati ripresi anche in COMMISSIONE DELLE COMUNITÀ EUROPEE, *Libro bianco. Un impegno comune per la salute: Approccio strategico dell'UE per il periodo 2008-2013*, Bruxelles, 23.10.2007, COM(2007) 630 definitivo.

Commissione perfezionò la Comunicazione "Sanità elettronica - migliorare l'assistenza sanitaria dei cittadini europei: piano d'azione per uno spazio europeo della sanità elettronica", nota anche come "*e-Health Action Plan*"[20]. Riconosciute le potenzialità degli strumenti digitali applicati al dominio sanitario e sottolineati i loro concreti benefici sia per gli operatori sia per i pazienti, fin dal suo *incipit* la Comunicazione preannuncia l'importanza di un cambio di prospettiva: incentrare i sistemi sanitari sul cittadino. Tenendo conto del ruolo crescente assunto dalle Tecnologie dell'Informazione e della Comunicazione e, peraltro, richiamando quanto già proposto nel piano d'azione "*eEurope 2005*", la Commissione considera quali strumenti idonei al raggiungimento di tale obiettivo la creazione di reti di informazione sanitaria, la costituzione di cartelle cliniche elettroniche, la diffusione di servizi di telemedicina, l'implementazione di sistemi di monitoraggio portatili ed indossabili, la predisposizione di portali istituzionali e tematici sulla salute.

Gli auspici della Commissione sono stati già in parte realizzati dai Paesi membri, e ciò, anche grazie ai significativi investimenti comunitari del quindicennio precedente che hanno permesso all'Europa di collocarsi in "una posizione dominante nell'utilizzo di cartelle cliniche elettroniche per l'assistenza sanitaria di base e nell'impiego di carte sanitarie elettroniche"[21].

Alla luce delle osservazioni esposte è, dunque, evidente il ruolo centrale che le nuove tecnologie assumono, sia nel facilitare l'accesso alle informazioni, sia nell'agevolare la collaborazione tra enti e professionisti. Soprattutto in un periodo storico, come quello attuale, caratterizzato da una forte mobilità internazionale, appropriatezza ed ottimizzazione dei processi di cura sono fondamentali per l'intero sistema socio-sanitario. In particolare, grazie alle cartelle sanitarie elettroniche, il personale designato ha la possibilità di accedere, in tempo reale, ai dati, e, quindi, è potenzialmente in grado di conoscere, in modo aggiornato e completo, la storia clinica del paziente, corredata da prognosi, diagnosi, indicazioni terapeutiche, immagini diagnostiche etc. Affinché tale ipotesi diventi realtà è, tuttavia, indispensabile implementare l'interoperabilità dei sistemi che, ad oggi, si manifesta ancora come nodo critico per i sistemi informativi sanitari.

---

[20] COMMISSIONE DELLE COMUNITÀ EUROPEE, *Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle Regioni, Sanità elettronica - migliorare l'assistenza sanitaria dei cittadini europei: piano d'azione per uno spazio europeo della sanità elettronica*, Bruxelles, 30.4.2004, COM (2004) 356 definitivo.

[21] Ivi, p. 4. E' altrettanto vero che il settore della sanità digitale presenta ancora diverse criticità ben motivate in A. A. ATIENZA et al., *Critical Issues in eHealth Research*, American Journal of Preventive Medicine, Vol. 32, Issue 5, Supplement, 2007, pp. S71-S74.

Se sono visibili i possibili benefici che il singolo utente può ricevere dalla digitalizzazione dei dati contenuti nelle cartelle sanitarie, anche sul fronte della pubblica amministrazione non mancano effetti positivi di tale innovazione, in termini di efficienza ed efficacia[22]. Significative in proposito le azioni intraprese dai Governi nazionali volte a ridurre la complessità dell'apparato burocratico, per migliorare tempi e qualità dell'erogazione dei servizi offerti all'utenza[23]. Altrettanto fondamentali gli interventi pubblici adottati per garantire la sicurezza dei sistemi informativi sanitari, grazie alla quale, utenti ed operatori sono incoraggiati all'utilizzo delle reti di comunicazione ed allo scambio dei dati sanitari, come, ad esempio, avviene in telemedicina[24]. Secondo quanto emerge da "*e-Health Action Plan*", nello scenario europeo sono presenti numerose applicazioni sviluppate nell'ambito della sanità digitale, in molti casi frutto di collaborazioni e finanziamenti (nazionali, comunitari ed internazionali) intercorsi nell'arco di un quindicennio[25].

Nonostante i miglioramenti introdotti dalle Tecnologie dell'Informazione e della Comunicazione, per molteplici cause, sono, però, ancora scarsi gli utilizzi degli strumenti di *e-Health*, soprattutto da parte degli utenti. Il *digital divide*, inteso sia come incapacità pratica di accedere alle nuove tecnologie - causata anche da una banda larga distribuita in modo non uniforme sul territorio nazionale - sia come ritardo socio-culturale per cui i cittadini europei raramente utilizzano servizi *online*, è certamente uno dei fattori che, insieme all'inadeguato stanziamento di risorse economiche e tecnologiche da parte delle

[22] Così come ad esempio sostenuto in A.S. KAZLEY, Y.A. OZCAN, *Organizational and environmental determinants of hospital EMR adoption: a national study*, Journal of Medical Systems, 31(5), 2007, pp. 375-84.

[23] Con preciso riferimento al contesto italiano, esempio concreto dell'interesse per la semplificazione e la digitalizzazione della P.A. sono l'attività oggi coordinata dalla "Agenzia per l'Italia Digitale", gestione ex DigitPA, le cui iniziative sono consultabili all'indirizzo http://www.digitpa.gov.it/, nonché il ruolo propulsivo svolto dal "Ministero per la pubblica amministrazione e la semplificazione" i cui interventi sono disponibili all'indirizzo http://www.funzionepubblica.gov.it/. L'ultima data di accesso a tutti i siti *web* richiamati nel presente lavoro è avvenuta il 29 maggio 2014.
L'ultimo accesso a tutti i siti *web* citati nel presente lavoro è avvenuto nel XXX.

[24] Inoltre, seppur con l'adozione di idonee misure di sicurezza per il trattamento dei dati personali e con la predisposizione di un *corpus iuris* comunitario *ad hoc*, i dati sanitari digitalizzati ed anonimi possono essere utilizzati per altre finalità, ad esempio quelle connesse alla ricerca clinico-diagnostica, all'epidemiologia, alla statistica e, più in generale, alle indagini di salute pubblica. Questo aspetto, sottolineato dalla Commissione nella citata Comunicazione del 2004, ha trovato in Italia un'importante applicazione nel maggio 2012 con la pubblicazione *online* da parte del Ministero della Salute di alcuni tipi di dati - per lo più trattasi di informazioni, dati numerici etc. -, disponibili in formato aperto e standardizzato, liberamente utilizzati, riutilizzati e distribuiti (c.d. *Open Data*).

[25] Nel capitolo successivo saranno, ad esempio, illustrati selezionati progetti, nazionali e non, riguardanti i fascicoli sanitari elettronici e resi appunto possibili sia dagli investimenti sia dalle politiche dell'Unione europea.

istituzioni territoriali, rallenta l'efficacia di tali mezzi[26]. A questo aspetto fa eco il tema dell'attuale scarsa fiducia dei consumatori nei potenti mezzi dell'era digitale. In proposito la Commissione europea si è già espressa più volte per incoraggiare gli Stati membri verso un rafforzamento di politiche e legislazioni nazionali, al fine di promuovere uno sviluppo omogeneo delle infrastrutture e dei mercati che, grazie a tali regole, potrebbero assistere ad una notevole crescita di domanda di beni e servizi fruibili nel *World Wide Web*.

Una forte sinergia tra i 27 Paesi è, dunque, l'auspicio sotteso all'intero Piano d'azione disegnato dalla Commissione europea. Affinché il mercato europeo della sanità digitale possa registrare *trend* positivi è, secondo la Commissione, necessario: stanziare maggiori finanziamenti per la ricerca in sanità elettronica; garantire maggiore certezza giuridica disciplinando i settori dell'assistenza sanitaria *online*, del diritto del lavoro su infortunistica e malattie professionali nonchè della responsabilità per i prodotti; sviluppare reti di informazione basate su infrastrutture fisse e senza filo, a banda larga e mobili, e sulle tecnologie GRID[27]; migliorare l'interoperabilità delle cartelle cliniche elettroniche. Altrettanto essenziale è, poi, accrescere la sensibilità e la cultura dell'utenza verso il tema dell'*e-Health*, ad esempio, attraverso interventi concreti di educazione sanitaria; a tal fine, sono decisivi la predisposizione di sistemi informativi accessibili, come siti *web* tematici sulla sanità pubblica, nonché la collaborazione tra gli Stati membri per la diffusione e condivisione di *best practice*.

3. VERSO UNA SOCIETÀ DELL'INFORMAZIONE *SICURA* ED *INTEROPERABILE*

Il profuso impegno ed il costante interesse della Commissione per il tema della nuove

[26] Tra gli altri, U. IZZO, P. GUARDA, *Sanità elettronica, tutela dei dati personali e digital divide generazionale. Ruolo e criticità giuridica della delega alla gestione dei servizi di sanità elettronica da parte dell'interessato*, Trento Law and Technology Research Group, Research Paper Series n. 3, 2010. Per maggiori approfondimenti sul tema del *digital divide* si rinvia a: A. J.A.M. VAN DEURSEN, *Internet skill-related problems in accessing online health information*, International Journal of Medical Informatics, Vol. 81, Issue 1, 2012, pp. 61-72; F. CRUZ-JESUS, T. OLIVEIRA, F. BACAO, *Digital divide across the European Union*, Information & Management, Vol. 49, Issue 6, 2012, pp. 278-291; D. CARVALHO, M. BESSA, L. OLIVEIRA, C. GUEDES, E. PERES, L. MAGALHÃES, *New Interaction Paradigms to Fight the Digital Divide: A Pilot Case Study Regarding Multi-Touch Technology*, Procedia Computer Science, Vol. 14, 2012, pp. 128-137; M.R. VICENTE, A.J. LÓPEZ, *Assessing the regional digital divide across the European Union-27*, Telecommunications Policy, Vol. 35, Issue 3, 2011, pp. 220-237; G.L. KREPS, L. NEUHAUSER, *New directions in eHealth communication: Opportunities and challenges*, Patient Education and Counseling, Vol. 78, Issue 3, 2010, pp. 329-336; M. BILLON, R. MARCO, F. LERA-LOPEZ, *Disparities in ICT adoption: A multidimensional approach to study the cross-country digital divide*, Telecommunications Policy, Vol. 33, Issues 10–11, 2009, pp. 596-610.

[27] In I. FOSTER, *The Anatomy of the Grid: Enabling Scalable Virtual Organizations*, International Journal of High Performance Computing Applications Fall, 2001, 15:200-222, i "*Grid computing*" o "sistemi Grid" sono definiti "*flexible, secure, coordinated resource sharing among dynamic collections of individuals, institutions, and resources - what is referred to as virtual organizations*".

Tecnologie dell'Informazione e della Comunicazione è confermato dalla "Comunicazione i2010 - Una società europea dell'informazione per la crescita e l'occupazione"[28], un vero e proprio piano strategico volto, da una parte, alla realizzazione di uno spazio unico europeo dell'informazione e di una società dell'informazione basata sull'inclusione, dall'altra, al rafforzamento dell'innovazione e degli investimenti nella ricerca delle TIC; tra i servizi pubblici *online* individuati dalla Commissione rientra l'assistenza sanitaria. La tipologia delle informazioni trattate in questo settore, forse più che in altri, richiede, però, un preciso intervento, volto a regolare le modalità di trattamento dei dati, oltre che dal punto di vista giuridico anche, e soprattutto, dal punto di vista tecnologico.

In questo contesto si colloca la Comunicazione "Una strategia per una società dell'informazione sicura. Dialogo, partenariato e responsabilizzazione"[29], in cui, al fine di fronteggiare le reali minacce alla sicurezza della società dell'informazione, si invita il settore privato ad "elaborare sistemi di certificazione della sicurezza a prezzi contenuti per prodotti, processi e servizi che rispondano ad esigenze comunitarie specifiche - in particolare in relazione alla vita privata"[30].

Nel maggio 2007, la Commissione europea, considerata la crescente diffusione di dati "sensibili" in Rete, preso atto dei nuovi rischi legati ad un uso distorto delle nuove tecnologie (quali, ad esempio, l'abuso della dignità altrui, forme di discriminazione, frodi informatiche etc.), riconosciuta la dimensione globale del fenomeno ed il conseguente coinvolgimento di una pluralità di giurisdizioni impegnate nella lotta alla criminalità informatica, ritenuta l'importanza di promuovere meccanismi tecnici e giuridici più stringenti, lancia la Comunicazione sulla "Protezione dei dati personali attraverso l'utilizzo delle *Privacy Enhancing Technology*" (PET)[31].

Punto di partenza di tale Comunicazione fu quanto già stabilito dall'articolo 17 della direttiva sulla protezione dei dati personali, il cui comma 1 prevede che: "gli Stati membri dispongono che il responsabile del trattamento deve attuare misure tecniche ed

---

[28] COMMISSIONE DELLE COMUNITÀ EUROPEE, *Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle Regioni, i2010 - Una società europea dell'informazione per la crescita e l'occupazione*, Bruxelles, 1.6.2005, COM(2005) 229 definitivo.

[29] COMMISSIONE DELLE COMUNITÀ EUROPEE, *Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, Una strategia per una società dell'informazione sicura. Dialogo, partenariato e responsabilizzazione*, Bruxelles, 31.5.2006, COM(2006) 251 definitivo.

[30] Ivi, p. 10.

[31] COMMISSIONE DELLE COMUNITÀ EUROPEE, *Comunicazione della Commissione al Parlamento europeo e al Consiglio sulla promozione della protezione dei dati mediante tecnologie di rafforzamento della tutela della vita privata (PET)*, Bruxelles, 2.5.2007, COM(2007) 228 definitivo. Al tema delle "*Privacy Enhancing Technology*" saranno dedicate alcune riflessioni specifiche nel corso del presente studio.

organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali. Tali misure devono garantire, tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere"[32]. Su questo aspetto, peraltro, la Commissione si era pronunciata anche con la direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche[33].

L'uso di misure tecniche volte a sostenere le regole legislative in materia di protezione dei dati personali, di cui il menzionato articolo 17 ben sintetizza taluni aspetti, era già stato, peraltro, promosso dalla Commissione europea nella "Prima relazione sull'applicazione della direttiva sulla tutela dei dati"[34], in cui il tema delle "*Privacy Enhancing Technology*" era stato oggetto di un particolare approfondimento. Scopo principale degli invocati strumenti tecnologici (tra cui ad esempio rientrano l'anonimizzazione automatica dei dati, gli strumenti crittografici, le *Platform for Privacy Preference*) è quello di garantire la tutela effettiva della vita privata degli utenti in conformità a quanto prescritto dalle norme sulla protezione della *privacy*, accrescendo anche la trasparenza e la fiducia degli utilizzatori[35]. Contestualmente all'implementazione delle PET è, tuttavia, necessario creare un solido *framework* giuridico sulla protezione dei dati personali, che individui obblighi e responsabilità degli attori coinvolti nel processo di acquisizione, trattamento e conservazione dei dati.

Nella citata Comunicazione del 2007, la Commissione indica azioni ed obiettivi concreti volti a perseguire una maggiore diffusione delle "*Privacy Enhancing Techonology*". Tra essi rientrano: (*a*) identificazione dei requisiti tecnologici necessari all'uso delle PET e loro

---

[32] *Ex* art. 17, comma I, *Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, pubblicata in GUCE n. L 281 del 23.11.1995.

[33] *Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)*, pubblicata in GUCE n. L 201/37 del 31.07.2002.

[34] COMMISSIONE DELLE COMUNITÀ EUROPEE, *Prima relazione sull'applicazione della direttiva sulla tutela dei dati (95/46/EC)*, Bruxelles, 15.5.2003, COM(2003) 265 definitivo.

[35] La Commissione europea cita in proposito le conclusioni contenute in ARTICOLO 29 - GRUPPO DI LAVORO PER LA TUTELA DEI DATI PERSONALI, *Documento di lavoro. Tutela della vita privata su Internet - Un approccio integrato dell'EU alla protezione dei dati on-line adottato il 21 novembre 2000*, 5063/00/IT/DEF.WP 37.

sviluppo, inteso come effettiva adozione e non soltanto progettazione; (*b*) diffusione dell'uso delle PET da parte dei detentori dei dati, e, in particolare, promozione dell'uso delle PET da parte dell'industria IT e delle autorità pubbliche[36], adozione di *standard* appropriati per la protezione dei dati personali attraverso l'uso delle PET nonché coordinamento delle legislazioni nazionali sul tema delle regole tecniche per la protezione dei dati personali (di cui le *Privacy Enhancing Technology* sono parte); (*c*) incoraggiare l'uso delle PET da parte dei consumatori, accrescendo, così, la loro fiducia nell'uso degli *e-service* (spesso minata dai molteplici rischi legati alla scarsa protezione dei dati personali in Rete), grazie anche all'adozione di "sigilli *privacy*" rilasciati da enti autorizzati e certificati.

Il 17 luglio 2007, a conclusione della "*e-Health Conference*" e sulla scia di quanto già tracciato ne "*e-Health Action Plan*", i partecipanti redassero la dichiarazione "*e-Health in Europe: Succeeding Together. European Co-operation on Europe-wide Electronic Health Services*", con la quale, Stati membri e Commissione europea, si impegnarono ufficialmente ad implementare una *roadmap* per lo sviluppo di servizi di sanità digitale transnazionali.

La Dichiarazione sintetizza le sei azioni da perseguire al fine di raggiungere un *framework* comunitario sull'interoperabilità: (i) facilitare la mobilità di pazienti e personale sanitario in Europa, anche grazie al supporto di mirati provvedimenti legislativi; (ii) organizzare una solida cooperazione tra gli Stati sui temi della protezione dei dati personali e degli *standard* nel campo della sanità elettronica; (iii) costruire dei piani d'azione nazionali sui temi della sanità elettronica, con particolare attenzione ai profili dell'interoperabilità dei sistemi sanitari e della messa in atto dei fascicoli sanitari elettronici; (iv) creare servizi di sanità digitale innovativi; (v) sollecitare iniziative integrate sui fronti degli *standard* e della sicurezza nel dominio in esame; (vi) coinvolgere e supportare l'industria e gli *stakeholder*.

Significativo a questo punto menzionare il Rapporto "*Accelerating the Development of the e-Health Market in Europe*"[37], pubblicato dalla Commissione europea nel 2007, il cui principale obiettivo fu quello di dare un nuovo impulso al mercato dell'*e-Health*, caratterizzato da un aumento della domanda di beni e servizi. Infatti, nonostante il *trend* positivo, diversi ostacoli impediscono una crescita più rapida della sanità elettronica; tra

[36] Su questo punto vedasi anche COM (2003) 567 def. già richiamata.
[37] EUROPEAN COMMISSION, *Accelerating the Development of the eHealth Market in Europe*, Brussel, 2007, pp. 36

essi, la frammentazione e la mancanza di interoperabilità (tecnica e semantica), l'insufficiente disponibilità di risorse finanziarie per fronteggiare la criminalità e le frodi informatiche, l'assenza di certezza giuridica nell'applicazione delle legislazioni in tema di protezione dei dati personali, rimborso per prestazioni mediche transfrontaliere e mobilità dei pazienti, responsabilità civile per il funzionamento difettoso dei beni.

Nel Rapporto del 2007 vengono annoverate concrete iniziative che testimoniano l'importante ruolo di supporto agli Stati membri svolto dalla Commissione europea proprio per il superamento dei *deficit* che impediscono un pieno sviluppo del settore: all'interoperabilità dei sistemi è, ad esempio, dedicato il "Programma di Innovazione e Competitività", e per azioni sul fronte della sicurezza e della *privacy* sono predisposti co-finanziamenti derivanti da "*Seventh EU Research Framework Programme*"[38].

I profili giuridici dell'*e-Health* sono esaminati, in dettaglio, nel Rapporto "*Legally e-Health - Putting e-Health in its European Legal Context*"[39], pubblicato nel 2008, dal quale emerge l'attenzione per la protezione ed il trattamento dei dati personali. Se il *framework* comunitario nel suo complesso fornisce delle risposte alle fattispecie sorte, al contempo è indiscussa la necessità di provvedere, con ulteriori disposizioni, ad una maggiore certezza normativa a favore di tutti gli attori coinvolti nell'*e-Health*; ancora una volta, tra le priorità rientra una maggiore interoperabilità transnazionale dei fascicoli sanitari elettronici, già auspicata ne "*e-Health Action Plan*".

Per rispondere all'esigenza di migliorare la connettività tra persone, sistemi e servizi all'interno dell'Unione, riducendo così il forte divario comunicativo instauratosi tra gli Stati membri a causa della mancanza di interoperabilità tra i sistemi informativi sanitari, il 2 luglio 2008 fu pubblicata la "Raccomandazione della Commissione sulla interoperabilità transfrontaliera dei sistemi di fascicoli sanitari elettronici"[40]. Benefici dell'interoperabilità, e, quindi, del flusso di dati sensibili dei pazienti all'interno dell'Unione, sono, anzitutto, la rapida accessibilità delle informazioni clinico-sanitarie del paziente ed il conseguente innalzamento della qualità e della sicurezza nelle cure[41]. Ulteriori vantaggi

---

[38] Per approfondimenti su "*Seventh EU Research Framework Programme*" si rinvia all'*homepage* del sito "*Community Research and Development Information Service*", consultabile all'indirizzo http://cordis.europa.eu/fp7/home_en.html.

[39] C. VAN DOOSSELAERE ET AL., *Legally eHealth: putting eHealth in its European legal context, study report on behalf of DG Information Society and Media*, European Commission, March, 2008.

[40] COMMISSIONE DELLE COMUNITÀ EUROPEE, *Raccomandazione della Commissione sulla interoperabilità transfrontaliera dei sistemi di fascicoli sanitari elettronici*, Bruxelles, 02.07.2008, COM(2008) 3282 definitivo.

[41] In conformità con quanto disposto dall'articolo 8 della "Convenzione sulla protezione dei diritti umani e delle libertà fondamentali", dall'articolo 8 della "Carta dell'Unione europea sui diritti fondamentali" nonché dalle direttive 95/46/EC e 2002/58/EC, la natura "sensibile" dei dati in esame richiede anche l'adozione di

dell'interoperabilità - organizzativa, semantica e tecnica - investono anche il personale sanitario, gli enti finanziatori, le agenzia assicurative, l'industria *IT* specializzata nel settore medico, il mercato dell'*e-Health*, l'*e-Government* ed i servizi pubblici fruibili in Rete. La Commissione europea, attraverso la citata Raccomandazione, intende fornire agli Stati membri linee guida utili al conseguimento dei risultati auspicati entro il 2015, senza, al contempo, minare l'autonomia nazionale di ciascun Paese. I concetti di interoperabilità e di armonizzazione dei sistemi sanitari sono, infatti, tra loro distinti ed il raggiungimento del primo non necessariamente implica la realizzazione del secondo, per il quale, invece, la sovranità nazionale è assoluta. Nel rispetto del principio di sussidiarietà, ogni Governo ha il compito ed il dovere di garantire il diritto di accesso dei propri cittadini alla salute, predisponendo mezzi efficienti ed efficaci, di cui un adeguato impianto normativo condiviso tra gli Stati membri è parte essenziale. Un significativo contributo all'integrità dei sistemi è, poi, dato dalle nuove tecnologie. Analogamente a quanto già proposto, anche in questa circostanza, la Commissione raccomanda l'uso delle *Security and Privacy Enhancing Technology* nella progettazione dei sistemi dedicati ai fascicoli sanitari elettronici. Spetta, dunque, agli Stati membri operare seguendo gli indicati livelli di azione: (i) legislativo, facilitando l'armonizzazione ed il coordinamento degli apparati normativi nazionali; (ii) organizzativo, creando un dominio condiviso tra i 27 Paesi e al tempo stesso assicurando l'autonomia nazionale quanto alla scelta di infrastrutture e di servizi di *e-Health*; (iii) tecnico, promuovendo l'uso di *standard*, architetture ed una piattaforma comune di interoperabilità, e semantico, coordinando le azioni nazionali; (iv) educativo, orientando verso l'adozione di adeguate misure volte a conseguire risultati elevati.

4. "EUROPA 2020": PRIORITÀ E STRATEGIE EUROPEE PER L'*E-HEALTH*

Nel marzo 2010, per rafforzare la crescita dell'Unione fortemente provata dalla crisi economico-finanziaria mondiale diffusasi nel biennio precedente, la Commissione europea lancia una nuova sfida attraverso la Comunicazione "Europa 2020. Una strategia per una crescita intelligente, sostenibile e inclusiva"[42], il cui scopo principale è guidare gli Stati Membri verso uno sviluppo collettivo che li impegni su precisi fronti, tra cui l'occupazione, la ricerca e l'innovazione, il cambiamento climatico e l'energia, l'istruzione e la lotta contro la povertà. Per favorire il raggiungimento dei risultati a livello nazionale,

rigide ed efficaci misure di sicurezza volte alla loro protezione, e ciò soprattutto per evitare usi impropri o addirittura illegali.

[42] COMMISSIONE EUROPEA, *Comunicazione della Commissione Europea 2020, Una strategia per una crescita intelligente, sostenibile e inclusiva*, Bruxelles, 3.3.2010, COM(2010) 2020 definitivo.

nonostante la forte eterogeneità in termini di sviluppo che caratterizza i Paesi dell'Unione, la Commissione individua sette iniziative guida, realizzabili anche attraverso un forte partenariato tra tutte le istituzioni coinvolte e la società civile. Ai fini del presente lavoro è di particolare interesse la predisposizione di una Agenda europea del digitale, volta ad "accelerare la diffusione dell'internet ad alta velocità e sfruttare i vantaggi di un mercato unico del digitale per famiglie e imprese"[43]. Il contesto che muove la Commissione a spendere risorse in questo settore è legato, anzitutto, all'inferiore quantità di investimenti europei nel campo dell'innovazione (rispetto a quanto, invece, accade in Giappone e negli Stati Uniti), e, di conseguenza, alla scarsa capacità dell'Unione europea di soddisfare il mercato del digitale. Inoltre, l'assenza di una copertura a banda larga, omogenea ed uniforme, nei territori nazionali nonché i considerevoli livelli di *digital divide* riscontrati, rallentano la diffusione e l'accesso a beni e servizi erogati attraverso i canali presenti in Rete.

I compiti individuati nella Comunicazione "Europa 2020" riguardano, pertanto, sia il fronte comunitario sia quelli nazionali. Quanto al primo, la stessa Commissione si impegna a: (i) creare un quadro giuridico che incentivi gli investimenti per la realizzazione di un'infrastruttura adeguata per l'Internet ad alta velocità; (ii) erogare fondi strutturali comunitari per il raggiungimento degli obiettivi di cui in Agenda; (iii) favorire un mercato unico per i contenuti ed i servizi digitali, sostenuto anche da un quadro normativo chiaro in materia di diritti, promozione delle licenze multiterritoriali, tutela e remunerazione adeguate per i titolari di diritti ed attivo sostegno per la digitalizzazione del patrimonio culturale europeo; (iv) riformare i fondi per la ricerca e l'innovazione e stimolare l'innovazione in materia di TIC in tutti i settori aziendali; (v) promuovere l'accesso alla Rete di tutti i cittadini europei anche attraverso azioni di alfabetizzazione. Per quanto, invece, riguarda il compito degli Stati membri, essi sono chiamati a realizzare l'Internet ad alta velocità sia attraverso la destinazione di fondi pubblici sia attraverso un quadro legislativo che consenta di ridurre i costi di ampliamento della Rete. Secondo la Commissione è, inoltre, necessario che i Governi si impegnino concretamente a diffondere servizi *online*.

Il 26 agosto 2010, ottemperando a quanto stabilito nella Comunicazione di marzo, la

[43] Ivi, p. 4.

Commissione europea lancia la Comunicazione "Agenda Digitale Europea"[44], allo scopo di "ottenere vantaggi socioeconomici sostenibili grazie a un mercato digitale unico basato su internet veloce e superveloce e su applicazioni interoperabili"[45]. Tale realtà è possibile grazie all'innescarsi di un circolo virtuoso dell'economia digitale, nel quale il rapporto tra l'offerta di una Rete veloce e l'erogazione di servizi *online* non soltanto è in sé crescente, ma genera un'ulteriore domanda di reti e servizi da parte degli utenti. Tuttavia, affinché la dinamica descritta si sviluppi secondo logiche di mercato che tutelino i consumatori, occorrono adeguati interventi normativi, comunitari e nazionali, che, da una parte, accrescano la fiducia degli utenti in termini di riservatezza e sicurezza nell'uso di Internet, dall'altra, permettano ai consumatori un regolare accesso, non gravoso o oneroso. Contestualmente al piano legislativo - osserva la Commissione - è indispensabile eliminare o, comunque, contenere tutti gli ostacoli che incidono negativamente sullo sviluppo di un mercato fortemente incentrato sul potenziale delle Tecnologie dell'Informazione e della Comunicazione, ostacoli individuabili in frammentazione dei mercati digitali, scarsa interoperabilità, aumento della criminalità informatica e rischio di un calo della fiducia nelle reti, inadeguati investimenti nelle reti, insufficiente stanziamento di fondi in ricerca e innovazione, assenza di alfabetizzazione digitale e competenze informatiche, scarse risposte ai problemi sociali.

Obiettivo principale della "Agenda Digitale Europea" è, dunque, individuare azioni e programmi che permettano di affrontare e risolvere i problemi sottesi alle aree summenzionate. Particolarmente interessanti per il presente studio sono: "*l'azione fondamentale 4*" sulla fiducia nel digitale di cui, *in primis*, fa parte il riesame del quadro normativo dell'Unione sulla protezione dei dati personali, tema al quale è fortemente legato il principio "*Privacy by Design*"[46]; "*l'azione fondamentale 5*" sull'interoperabilità tra prodotti e servizi delle tecnologie dell'informazione possibile, anzitutto, grazie all'introduzione di strumenti giuridici *ad hoc* che modifichino le regole sull'applicazione degli *standard* europei in materia di Tecnologie dell'Informazione e della Comunicazione; "*le azioni fondamentali 13 e 14*" rispettivamente dedicate a garantire, a tutti i cittadini europei, "un accesso *online* sicuro ai dati sanitari personali entro il 2015 e diffondere ampiamente i servizi di telemedicina entro il 2020" nonché a "proporre una

[44] COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni "Un'agenda digitale europea"*, Bruxelles, 26.8.2010, COM(2010) 245 definitivo/2.
[45] Ivi, p. 3.
[46] I principi della "*Privacy by Design*" e le loro applicazioni saranno esaminati nel corso della ricerca.

raccomandazione per definire un numero minimo comune di dati sui pazienti per garantire l'interoperabilità delle cartelle cliniche che dovranno essere accessibili o scambiabili per via elettronica fra gli Stati membri entro il 2012"[47].

Il tema della sanità elettronica acquista un ruolo particolarmente importante anche per le questioni sottese all'assistenza sanitaria oltre i confini nazionali, cresciuta, negli ultimi anni, soprattutto per la forte mobilità internazionale dei cittadini. Questa la ragione che ha spinto il legislatore comunitario ad introdurre l'articolo 14, rubricato "assistenza sanitaria *online*", nella direttiva 2011/24/UE sull'assistenza sanitaria transfrontaliera[48]. Gli obiettivi della norma invocata corrispondono, peraltro, a quelli esposti dalla Commissione europea in altre Comunicazioni già esaminate. Nelle disposizioni del 2011 sono, in particolare, sottolineati l'utilità di *network* transfrontalieri nell'assistenza sanitaria *online* e di sistemi interoperabili sia per la continuità sia per la qualità delle cure prestate nonché, nel rispetto di quanto previsto dalle direttive 1995/46/CE e 2002/58/CE in materia di protezione dei dati personali, la necessità di delineare precise indicazioni sui "dati che devono essere inseriti nei fascicoli dei pazienti e che possano essere scambiati tra professionisti sanitari per garantire la continuità delle cure e la sicurezza del paziente a livello transfrontaliero" e sui "metodi efficaci per consentire l'uso di informazioni mediche per la sanità pubblica e la ricerca". É, altresì, disposto di "sostenere gli Stati membri affinché definiscano misure comuni di identificazione ed autenticazione per agevolare la trasferibilità dei dati nell'assistenza sanitaria transfrontaliera" (così prescrive l'articolo 14, secondo comma, lettere *b)* e *c)*).

5. LE STRATEGIE NAZIONALI DEGLI STATI MEMBRI

Le risposte alle priorità ed alle strategie europee in materia di *e-Health* da parte degli Stati membri dell'Unione non sono tardate. Seppur non in modo congiunto, infatti, i Governi nazionali hanno tradotto in azioni concrete le indicazioni loro fornite dalla Commissione europea nei documenti, cogenti e non, di cui si è dato un rapido cenno nel corso della presente ricognizione sulle attuali tendenze politiche e giuridiche in tema di sanità digitale e fascicolo sanitario elettronico.

In particolare, secondo l'indagine conclusa nel marzo 2007 dal gruppo di lavoro

[47] COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni "Un'agenda digitale europea"*, p. 33.
[48] *Direttiva 2011/24/UE del Parlamento europeo e del Consiglio del 9 marzo 2011 concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera*, pubblicata in GUCE n. L 88/45 del 4.4.2011.

coordinato da *e-Health ERA*, successivamente al lancio de "*e-Health Action Plan*", la maggior parte dei 27 Paesi membri aveva redatto una propria strategia nazionale, fissando obiettivi, a medio e a lungo termine, attraverso i quali colmare anzitutto i *gap* che a livello nazionale avrebbero impedito un uso consolidato delle nuove tecnologie nel dominio sanitario, come, ad esempio, la scarsa diffusione della banda larga[49]. Inoltre, secondo quanto emerge dal Rapporto, sul tema della sanità elettronica alcuni Stati, trattasi in particolare di Danimarca, Finlandia e Norvegia, già dalla seconda metà degli anni Novanta avevano intrapreso politiche nazionali in materia di *e-Health*, e, negli stessi anni, la Germania iniziava un intenso dibattito sui medesimi argomenti con tutti gli *stakeholder* coinvolti.

Sebbene ciascun Paese abbia concretizzato in modo diverso il raggiungimento degli obiettivi di digitalizzazione in sanità, alcuni denominatori comuni, quali la qualità delle cure nonché l'efficacia e l'efficienza dei servizi offerti agli utenti, hanno, però, caratterizzato le politiche locali e gli impegni assunti dai sistemi sanitari nazionali. In ottemperanza alle indicazioni della Commissione, la logica, almeno teorica, che ha prevalso in Europa è stata, dunque, quella di preferire strumenti e servizi *patient-centred*.

Parallelamente allo sviluppo dell'impianto tecnologico - emerge dal Rapporto citato -, molti Governi, consapevoli dei rischi legati ai nuovi strumenti tecnologici, tra cui

---

[49] *Cfr*. ERA, *eHealth strategies and implementation in European countries. EHealth ERA Report*, Luxembourg, Office for Official Publications of the European Communities, 2007, pp. 100.
Nel presentare schede tecniche relative ai singoli Paesi esaminati, il Rapporto menziona, tra gli altri, i documenti nazionali che hanno permesso l'adozione di strategie, politiche ed azioni in tema di sanità elettronica. Al solo fine di dare riscontro sullo sviluppo dell'*e-Health* in Europa, di seguito si riportano (secondo un ordine cronologico e mantenendo la citazione in lingua inglese dell'*e-Health ERA Report*) i documenti fondamentali adottati dagli Stati oggetto dello Studio: "*The Strategy for the Utilisation of Information and Communication Technologies in Welfare and Health*" - 1996 (Finlandia), "*More health for each bIT*" - 1997 (Norvegia), "*The e-Health strategy*" - 2000 (Estonia), "*The New Healthcare Information System*" - 2001 (Italia), "*The National Action Plan eEurope+Czech Republic*" - 2002 (Repubblica Ceca), "*The National Programme for IT*" - 2002 (Inghilterra), "The *National Strategy for Information Technology in the Health Care System (2003 - 2007)*" - 2003 (Danimarca), "*Informing Healthcare*" - 2003 (Galles), "*National Health Information System*" - 2003 (Turchia), "*The National eHealth Programme*" - 2004 (Ungheria), "*Poland - eHealth Strategy for 2004 - 2006*" - 2004 (Polonia), "*The National Health Information Strategy*" - 2004 (Irlanda), "*The Healthcare Insurance Act of August 2004*" - 2004 (Francia), "*The National Healthcare servie's "Bricks*" - 2004 (Italia), "*The National Health Plan*" - 2004 (Portogallo), "*The eHealth strategy*" - 2005 (Romania), "*The eHealth2010 - Strategic plan for the Slovenian health sector informatisation*" - 2005 (Slovenia), "*The Health Reform 2005 Act*" (Austria), "*The DHSSPS Health and Personal Social Services Information and Communications Technology Strategy*" - 2005 (Irlanda del Nord), "*Health Telematic Law*" - 2005 (Belgio), "*The German eHealth Strategy*" - 2005 (Germania), "*e-Health in Latvia*" - 2005 (Lettonia), "*eHealth Strategy for 2005-2010*" - 2005 (Lituania), "*The National Strategy for Health of Bulgaria*" - 2006 (Bulgaria), "*The National Strategy for Quality and Safety of Healthcare Services in the Knowledge Society*" - 2006 (Grecia), "*The national eHealth Vision and strategy*" - 2006 (Malta), "*The National eHealth strategy*" - 2006 (Svezia), "*The Government Programme for 2005 - 2009*" - 2006 (Liechtenstein), "*A draft national strategy for eHealth*" - 2006 (Switzerland), "*The Plan for Quality in the National Health System*" - 2006 (Spain), "*New Healthcare System*" - 2006 (Slovacchia), 2006 (Olanda); "Delivering for Health", Islanda.

l'inadeguatezza in materia di protezione e trattamento dei dati personali, hanno predisposto precise misure legislative.

Anche dal punto di vista delle attività e dei progetti nazionali volti ad implementare le indicazioni formulate dalla Commissione europea, il Rapporto sottolinea che, al 2006, anno di aggiornamento dei dati pubblicati, le azioni intraprese erano piuttosto numerose e diversificate[50]. Tra gli ambiti di intervento citati rientrano, ad esempio, la predisposizione di infrastrutture, la realizzazione di fascicoli sanitari elettronici e di vari prototipi di *e-Card* nonché la messa in Rete di portali tematici.

Il raggiungimento di tutti i risultati auspicati non può, tuttavia, omettere precise azioni su altri profili, tra cui, l'interoperabilità tecnica e semantica nonché la sicurezza e l'identificazione personale dell'utente, riconosciuti essenziali sia da "*e-Health Action Plan*" sia dalla letteratura esistente.

Già all'epoca della redazione de "*e-Health ERA Report*", diverse iniziative nazionali erano state avviate per implementare i menzionati interventi. Per quanto riguarda il profilo dell'interoperabilità interessante notare che l'indagine confermi che soltanto alcuni Stati (Italia, Romania e Spagna) abbiano espressamente inserito questo concetto chiave indicato da "*e-Health Action Plan*" nella loro Agenda, attribuendo pertanto all'interoperabilità tecnica e semantica un ruolo prioritario; inoltre, la Danimarca, con il "Progetto MedCom", ha sviluppato una piattaforma, "*the Danish Health Data Network*", per *standard* tecnici e per l'interoperabilità di *e-Message*, e, attraverso il "Progetto SNOMED CT" ha cercato di realizzare in modo concreto l'interoperabilità semantica.

Rispetto ai profili giuridici in materia di *e-Health*, interessanti sono i risultati presentati nella ricerca condotta da Empirica, i cui risultati sono stati pubblicati ne "*European countries on their journey towards national e-Health infrastructures - e-Health Strategies Report*"[51].

Lo studio analizza lo stato dell'arte dei Paesi membri dell'Unione nella prospettiva delle indicazioni delineate dal Consiglio europeo ne "*e-Health Action Plan*" del 2004; sono, altresì, esaminate strategie e *policy*, normative, infrastrutture ed applicazioni adottati per ottemperare alle indicazioni del Consiglio europeo. Tra i risultati più evidenti rientra il reale impegno, assunto fino ad oggi, da parte di tutti gli Stati europei nel settore della sanità digitale, impegno, peraltro, dimostrato attraverso azioni intraprese proprio a seguito

[50] Si noti che lo stato dell'arte attualmente presenta la stessa eterogeneità.

[51] EMPIRICA, *European countries on their journey towards national eHealth infrastructures. eHealth Strategies Report*, 2011, pp. 47.

del Piano del 2004 e concretamente perseguite nel territorio dell'Unione. Ne sono esempi le Conferenze ministeriali annuali sull'*e-Health*, il "Progetto pilota epSOS (*Smart Open Services for European Patients*)"[52] nel quale sono coinvolti 23 Paesi europei nonché il "Progetto pilota *RenewingHealth*" sui servizi di telemedicina[53]. Monito fondamentale de "*e-Health Strategies Report 2011*" è, certamente, la cooperazione e la collaborazione sinergica tra gli Stati dell'Unione sui temi della sanità digitale, in riferimento ai profili tecnici (uso di *standard* per l'interoperabilità dei fascicoli sanitari elettronici), giuridici (tutela dei dati personali sanitari e responsabilità nel trattamento), politici, economico-finanziari. Le ragioni di tali conclusioni vanno tra l'altro ravvisate nel fatto che la mobilità internazionale dei cittadini/consumatori/pazienti europei richiede l'adozione di misure comuni e condivise tra i Paesi dell'Unione europea, soprattutto per migliorare la qualità delle prestazioni offerte e tutelare gli stessi beneficiari delle cure.

6. UNA SANITÀ INNOVATIVA PER IL 21ESIMO SECOLO: IL "PIANO D'AZIONE SANITÀ ELETTRONICA 2012-2020"

Come è stato osservato, nel maggio 2012, da Ilves, presidente della *task force* indipendente composta da esperti di alto livello in materia di sanità elettronica[54], nonostante gli sforzi compiuti dall'Unione europea e dai 27 Paesi membri per la digitalizzazione della sanità e dell'assistenza sanitaria, questo dominio rimane in notevole ritardo rispetto a molti altri settori, nei quali le modalità di organizzazione, erogazione e fruizione dei servizi sono strutturalmente permeate dall'uso delle Tecnologie dell'Informazione e della Comunicazione.

Tra gli ostacoli, a tutt'oggi esistenti, rientra certamente l'onere normativo, per i Governi ed i loro apparati burocratico-amministrativi, che spesso si manifesta come incertezza e frammentarietà del diritto e che impedisce, quindi, una migliore diffusione e fruibilità delle informazioni e delle prestazioni sanitarie; non secondaria rilevanza assumono, inoltre, questioni come il *digital divide* e lo scetticismo che talora persiste tra gli *stakeholder* di fronte all'uso degli strumenti di sanità elettronica nonché il tema dei costi, ancora eccessivamente elevati per la realizzazione di nuovi sistemi e prototipi.

---

[52] Per approfondimenti si rinvia all'*homepage* del Progetto "*epSOS*", consultabile all'indirizzo http://www.epsos.eu/.

[53] Il sito *web* del Progetto "*Renewing Health*" è disponibile all'indirizzo http://www.renewinghealth.eu/.

[54] Istituita nel maggio 2011 dalla Commissione, la *task force* ha avuto il compito di valutare le modalità con cui massimizzare i potenziali benefici derivanti dall'utilizzo delle nuove tecnologie nel settore sanitario. I risultati di tale lavoro sono stati raccolti nello studio EHEALTH TASK FORCE REPORT "*Redesigning health in Europe for 2020*", Luxemburg, 2012, pp. 12

Di fronte a questo scenario, l'auspicio non può che essere l'ulteriore sensibilizzazione, centrale e locale, per la rimozione degli ostacoli che danneggiano una collaborazione sinergica per il rilancio di un *e-Health* non soltanto formale ma soprattutto sostanziale. A questo scopo, il rapporto redatto dalla *task force*, "*Redesigning health in Europe for 2020*", individua cinque livelli per il cambiamento: 1) "*My data, my decisions*": evidenzia ancora una volta la centralità che, per i consumatori, assumono il diritto di decidere sull'accesso ai dati ed il diritto di ricevere un'informazione adeguata ed esaustiva sul trattamento dei dati stessi; 2) "*Liberate the data*": sottolinea l'importanza di "aprire" l'utilizzo (seppur con le dovute precauzioni di anonimizzazione) di dati raccolti in archivi diversi da quelli socio-sanitari per finalità di salute pubblica; 3) "*Connect up everything*": rinvia alla necessità di adottare sistemi informativi interoperabili, accessibili anche attraverso "*multi-platform apps*"; 4) "*Revolutionise health*": richiama l'opportunità di pubblicizzare le *performance* dei professionisti sanitari ed i risultati delle istituzioni sanitarie al fine di consentire agli assistiti di orientarsi verso servizi maggiormente all'avanguardia; 5) "*Include everyone*": sollecita gli erogatori dei servizi sanitari ad una lettura oggettiva dello stato dell'arte, nel quale, ancora, fasce diffuse di popolazione non dispongono degli strumenti idonei a fruire delle prestazioni in modalità digitale (*digital divide*). Altrettanto significativo menzionare le cinque "Raccomandazioni" rivolte dagli esperti alla Commissione europea: 1) "*A new legal basis for health data in Europe*"; 2) "*Create a 'beacon group' of Member States and regions committed to open data and eHealth*"; 3) "*Support health literacy*"; 4) "*Use the power of data*"; 5) "*Re-orient EU funding and policies*".

Per ottemperare al rilancio della digitalizzazione della sanità, già peraltro invocato dalla "Agenda Digitale Europea" e dal piano strategico "Europa 2020", e rispondere, quindi, alle nuove sfide nel settore della sanità elettronica, alla fine del 2012, la Commissione europea ha definito uno specifico piano d'azione, "Sanità elettronica 2012-2020 - Una sanità innovativa per il 21esimo secolo" (o "*eHealth Action Plan 2012-2020*")[55], i cui obiettivi operativi possono essere così sintetizzati: maggiore interoperabilità dei sistemi di sanità elettronica; ricerca, sviluppo ed innovazione nell'*e-Health* al fine di migliorare efficienza ed efficacia dei servizi offerti ai consumatori; promozione di un dialogo politico e di una cooperazione globale sul tema.

Ciò che emerge in modo predominante dal Piano d'azione in esame è la sollecitazione

[55] COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni "Piano d'azione "Sanità elettronica" 2012-2020 – Una sanità innovativa per il 21esimo secolo"*, Bruxelles, 6.12.2012, COM(2012) 736 definitivo.

ad una forte interazione tra tutti i soggetti a qualsiasi titolo coinvolti nelle dinamiche sanitarie, siano essi attori operanti a livello comunitario, siano essi attori operanti a livello nazionale, centrale o territoriale. Si osservi l'importanza di questa annotazione, più volte, peraltro, in passato già richiamata dalle istituzioni europee; un approccio di tal genere è, infatti, imprescindibile in un settore multilivello e multidisciplinare come quello dell'*e-Health*, soprattutto per ottenere risultati il più possibile integrati e coordinati.

Particolarmente significativo ai fini della presente ricerca è, altresì, il monito della Commissione europea per la creazione di un quadro europeo interoperabile - dal punto di vista giuridico, organizzativo, semantico e tecnico - in materia di sanità elettronica.

Per quanto concerne gli aspetti semantici e tecnici, precipua attenzione è rivolta non soltanto all'utilizzo di *standard* e specifiche europee ed internazionali di cui, tra l'altro, si riferirà nel capitolo seguente, ma anche "le prove di interoperabilità nonché i processi di etichettatura e certificazione"[56].

Per quanto, poi, i profili legali, la Commissione osserva che "rimuovere gli ostacoli giuridici è di importanza cruciale per la diffusione della sanità elettronica in Europa"[57]; da qui, l'opportunità di dar vita a gruppi di studio ed attività intersettoriali, che affrontino questioni quali la revisione delle norme sulla protezione dei dati personali, in cui, peraltro, non possono essere ignorate nuove fattispecie concrete nate dalla sempre più diffusa applicabilità delle TIC anche al settore sanitario (tra le altre, si consideri, ad esempio, la possibilità di raccogliere e trattare i dati sanitari in infrastrutture e servizi di *cloud computing* o nei dispositivi "*mobile*").

[56] *Cfr*. COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni "Piano d'azione "Sanità elettronica" 2012-2020 – Una sanità innovativa per il 21esimo secolo"*, p. 9.
[57] *Idem*.

CAPITOLO II

IL FASCICOLO SANITARIO ELETTRONICO NELLO STATO DELL'ARTE EUROPEO ED ITALIANO

SOMMARIO: 1. Il Fascicolo Sanitario Elettronico - 2. Il sistema informativo sanitario: brevi cenni - 3. Il processo di standardizzazione in sanità - 4. Analisi di selezionati progetti europei e nazionali - 4.1 Unione europea - 4.1.1 Progetto "*epSOS*" - 4.2 Austria - 4.2.1 Progetto "*ELGA*" - 4.2.1.1 "*Integrating the Healthcare Enterprise Integration Profiles*" - 4.2.1.2 "*HL7 Reference Information Model*" e "*HL7 Clinical Documentation Architecture*" - 4.2.1.3 "*eXtensible Access Control Markup Language*" - 4.2.1.4 Architettura Progetto "*ELGA*" - 4.3 Danimarca - 3.3.1 Progetto "*MedCom*" - 4.4 Italia - 3.4.1 Progetto "*InFSE*" - 4.4.1.1 Progetto "*OpenInFSE*" - 4.4.1.2 Progetto "*Evoluzione e interoperabilità tecnologica del Fascicolo Sanitario Elettronico*" - 4.4.2 Progetto "*IPSE*"

1. IL FASCICOLO SANITARIO ELETTRONICO

Multidisciplinarietà ed interdisciplinarietà caratterizzano la sanità digitale; numerose sono, infatti, le branche del sapere coinvolte: medicina, ingegneria biomedica e gestionale, informatica, diritto, bioetica, sociologia, economia, politica, per citarne alcune. Per queste ragioni, il dibattito scientifico è particolarmente vivace e ricco di nuovi scenari e prospettive: sui fronti teorico ed applicativo si assiste, infatti, al moltiplicarsi di posizioni ed azioni tra loro complementari o talora discordanti.

Detta complessità impone di tracciare, seppur senza alcuna pretesa di esaustività, i principali elementi dello strumento di *e-Health* oggetto del presente studio, il Fascicolo Sanitario Elettronico[58]. A tal fine saranno considerati selezionate pubblicazioni presenti in letteratura, documenti tecnici internazionali e nazionali elaborati da gruppi di lavoro ed esperti della materia nonché significativi progetti realizzati a livello comunitario e nazionale.

Se il quadro politico e legislativo dell'ultimo decennio, tratteggiato nel capitolo precedente, rivela l'interesse e l'attenzione della Commissione europea per la sanità digitale, al tempo stesso quanto delineato mostra l'attuale divenire degli scenari normativi. Come già sottolineato, le ragioni di tale progressività sono, tra l'altro, dovute alla

[58] Nel presente lavoro i termini Fascicolo Sanitario Elettronico ed *Electronic Health Record* sono utilizzati come sinonimi.

farraginosità degli apparati legislativi ed amministrativi che, di frequente, richiedono tempi di revisione maggiori rispetto alle innovazioni introdotte dalle nuove tecnologie in altri ambiti scientifici.

In campo medico le prime forme di "*Electronic Health Record*" (EHR) furono utilizzate negli Stati Uniti già a partire dagli anni Sessanta[59]. Sebbene questo dato sia particolarmente significativo, poiché sottolinea che da oltre un cinquantennio ci si occupa degli aspetti architetturali ed infrastrutturali dei fascicoli sanitari elettronici, attualmente sono ancora parecchi gli ostacoli da superare per raggiungere i livelli di interoperabilità - organizzativa, tecnica, semantica - auspicati dalla Commissione europea[60], e ciò, soprattutto per il fatto che in Europa è spesso mancata una visione unitaria e condivisa nell'adozione ed implementazione di *standard* volti a migliorare l'efficienza e l'efficacia dei sistemi stessi. Inoltre, in paesi come l'Italia, ulteriori ostacoli all'interoperabilità semantica sono conseguenza di un'inefficace strutturazione di dati e documenti sanitari digitali, ancora troppo spesso legata all'analogo modello formale cartaceo.

Nonostante questi dati, come mostra lo stato dell'arte, la mobilità nazionale ed internazionale dei consumatori è, sempre più, fattore trainante per la revisione dei servizi sanitari nazionali tradizionali, al punto che, soprattutto nell'ultimo decennio, a livello dei "sistema Paese", sono stati predisposti programmi operativi per costituire o, comunque, implementare infrastrutture orientate all'interoperabilità[61].

Prima di esaminare in che modo la realtà considerata si stia modificando e ridisegnando, occorre, anzitutto, ripercorrere la letteratura specialistica per delineare le fondamentali

---

[59] Tra gli altri: R. DICK, E. B. STEEN, D. DETMER (eds.), *The Computer Based Patient Record: An Essential Technology for Health Care*, Institute of Medicine, National Academy Press, 1997, p. 111; A. B. SUMMERFIELD, E. EMPEY, *Computer-based Information Systems for Medicine: A Survey and Brief Discussion of Current Projects*, Santa Monica, Calif.: Systems Development Corporation, 1965.

[60] *Cfr*. COMMISSIONE DELLE COMUNITÀ EUROPEE, *Raccomandazione della Commissione del 2 luglio 2008 sull'interoperabilità transfrontaliera dei sistemi di cartelle cliniche elettroniche* [notificata con il numero C(2008) 3282] (2008/594/CE), pubblicata in GUCE L 190/37 del 18.7.2008. Vedasi, altresì, IDABC, EUROPEAN INTEROPERABILITY FRAMEWORK, *European Interoperability Framework for Pan European eGovernment Services*, version 1.0, Luxemburg, 2004, pp. 26; altrettanto valida è, poi, la definizione di interoperabilità in N. BROWN, M. REYNOLDS, *Strategy for production and maintenance of standards for interoperability within and between service departments and other healthcare domains. Short Strategic Study CEN/TC251/N00-047*, CEN/TC 251 Health Informatics, Brussels, Belgium, 2000).

[61] Un significativo esempio è il progetto europeo "epSOS". Interessanti in proposito anche i risultati degli studi: A. DOBREV, T. JONES, V. STROETMANN, K. STROETMANN, Y. VATTER, K. PENG, *Interoperable eHealth is Worth it. Securing Benefits from Electronic Health Records and ePrescribing. Study Report 2010*, European Communities, Bonn/Brussels, 2010, pp. 88; A. DOBREV, T. JONES, K. STROETMANN, Y. VATTER, K. PENG, *Report on The socio-economic impact of interoperable electronic health record (EHR) and ePrescribing systems in Europe and beyond. Final study report*, Deliverable D3.4 of the EHR IMPACT study, 2009, pp. 54. Altrettanto significativi i risultati di uno studio condotto per valutare la qualità dei modelli di EHR diffusi negli ultimi anni negli Stati Uniti e in Europa: A. HOERBST, E. AMMENWERTH, *Quality and Certification of Electronic Health Records. An overview of current approaches from the US and Europe*, Applied Clinical Informatics, 2010, pp. 149-164.

caratteristiche del Fascicolo Sanitario Elettronico. Il motivo principale va rintracciato, più che in ragioni meramente semantiche, in finalità pragmatiche: non tutti i termini utilizzati per indicare il Fascicolo Sanitario Elettronico si riferiscono, infatti, al medesimo strumento[62]. A titolo esemplificativo, "*Electronic Medical Record*", "*Patient Summary*", "*e-Prescribing*", "*Patient Health Record*" soltanto per i non addetti ai lavori rinviano allo stesso concetto di "cartella sanitaria"; nella prassi, essi rimandano a prototipi digitali differenti, sia per caratteristiche tecniche ed architetturali sia per i possibili usi.

Particolarmente significativo è in tal senso il *dossier* redatto da *International Organization for Standardization* (ISO) nel 2005, nel quale, utilizzando un approccio per così dire multilivello, una delle principali organizzazioni mondiali nel campo della standardizzazione ha dedicato speciale attenzione proprio al tema del Fascicolo Sanitario Elettronico[63].

Le definizioni proposte da ISO, più che tener conto dei contenuti di questo strumento digitale, si basano sulla struttura dello stesso. L'idea principale è, infatti, quella di pensare alla cartella sanitaria elettronica alla luce dei suoi possibili usi, generico o specialistico.

Nel suo uso generico il Fascicolo Sanitario Elettronico si presenta come raccolta di informazioni clinico-sanitarie riferibili ad un paziente e leggibili da supporti informatici[64]. Ciò che, invece, differenzia i due modelli specialistici ("*non shareable*" e "*shareable*") è l'interoperabilità, qui intesa come l'idoneità tecnica e/o architetturale di un Fascicolo Sanitario Elettronico di scambiare informazioni tra pluralità di utenti, pluralità di applicazioni, pluralità di sistemi.

Almeno dal punto di vista formale, prototipo ideale della descritta interoperabilità è, secondo ISO, "*integrated care EHR*", un sotto-tipo di "*shareable EHR*", le cui peculiarità sono l'interoperabilità semantica, la completezza e la persistenza di informazioni riguardanti la storia clinica del paziente, l'adozione di modelli logici standardizzati che travalicano i sistemi fisici locali nonché la sicurezza nella trasmissione delle informazioni e l'accessibilità alle stesse per i soli soggetti autorizzati[65].

A conferma della tesi innanzi esposta, secondo cui l'espressione "Fascicolo Sanitario Elettronico" non indica in modo univoco le caratteristiche tecniche di uno strumento

---

[62] In proposito *cfr.* K. HÄYRINEN, K. SARANTO, P. NYKÄNEN, *Definition, structure, content, use and impacts of electronic health records: A review of the research literature*, International Journal of Medical Informatics, vol. 77, 2008, pp. 291-304.

[63] INTERNATIONAL STANDARDIZATION ORGANIZATION, *Health informatics - Electronic health record - Definition, scope, and context*, 2005, ISO/TR 20514:2005(E).

[64] Ivi, p. 8. Analoga definizione era, peraltro, già stata delineata dall'ISO nel documento ENV 13606-1:2000.

[65] Ivi, p.10.

digitale finalizzato alla raccolta di informazioni clinico-sanitarie, è di aiuto il citato *dossier*, nel quale, *International Standardization Organization* presenta una rassegna dei vari tipi di "cartelle sanitarie", utilizzati dai sistemi sanitari nazionali nonostante l'assenza di standardizzazione. Tra essi rientrano: "*Electronic Medical Record*" (EMR), un fascicolo sanitario elettronico la cui peculiarità è essere "*medically focused*"; "*Electronic Patient Record*" (EPR), la cui gestione è limitata ad una singola struttura sanitaria; "*Electronic Client Record*" (ECR), un fascicolo sanitario elettronico le cui informazioni sono utilizzate nel contesto delle attività svolte da professionisti non medici del settore sanitario, come fisioterapisti, chiropratici o operatori sociali.

Maggiormente articolata è, poi, la definizione di "*Personal Health Record*" (PHR), di cui, secondo ISO, è possibile individuare almeno quattro differenti forme: "*a) a self-contained EHR, maintained and controlled by the patient/consumer, b) the same as a. but maintained by a third party such as a web service provider, c) a component of an ICEHR maintained by a health provider (e.g. a GP) and controlled at least partially (i.e. the PHR component as a minimum) by the patient/consumer, or d) the same as c) but maintained and controlled completely by the patient/consumer*".

Secondo quanto emerge dal documanto citato, altrettanto diffusi sono, inoltre, "*Digital Medical Record*" (DMR), cartella "*web-based*", gestita dal servizio sanitario, che può assolvere funzioni di EMR, EPR o EHR[66] e "*Clinical Data Repository*" (CDR), nel quale i dati sanitari provenienti dai servizi sanitari territoriali, come ospedali o cliniche, sono contenuti ed organizzati, dati che possono anche alimentare il Fascicolo Sanitario Elettronico.

Altri modelli adottati dai sistemi sanitari nazionali sono, infine, "*Computerised Medical Record*" (CMR), nel quale la documentazione raccolta nelle cartelle sanitarie cartacee è acquisita mediante i sistemi ottici di riconoscimento dei caratteri[67] e "*Population Health Record*" (PHR), creato *ex novo* o generato direttamente dai fascicoli sanitari elettronici, nel quale, invece, dati aggregati, e comunque resi anonimi, sono utilizzati in sanità pubblica[68].

Una prima osservazione di carattere generale riguarda la titolarità nella gestione delle informazioni sanitarie: soltanto nel "*Patient Health Record*" i dati sono di fatto generati dal paziente. Questo elemento è assunto nella sua oggettività; nella presente ricerca sono, infatti, omesse ulteriori considerazioni ed implicazioni. Si evidenzia, a titolo

[66] Tale definizione è stata ripresa da P. WAEGEMANN, *Status Report 2002: Electronic Health Records*, Medical Records Institute, 2002.
[67] P. WAEGEMANN, *cit.*
[68] Ivi, pp. 12-14.

esemplificativo, che l'assenza di adeguate conoscenze mediche da parte dei fruitori dell'assistenza sanitaria e l'uso di un linguaggio spesso inappropriato nella descrizione della sintomatologia, possono condizionare negativamente la qualità delle cure e la scelta delle migliori forme di assistenza per il paziente da parte dei medici designati. Ulteriori importanti scenari riguardano poi i profili di compatibilità ed interoperabilità tra dispositivi mobili utilizzabili dal paziente ed i fascicoli sanitari elettronici gestiti dal personale sanitario. Seppur tratteggiati alcuni dei limiti che i *personal device* presentano, non si può, al tempo stesso, non sottolineare il valore che essi hanno in termini di innovazione dei sistemi sanitari tradizionali e, particolarmente, il contributo che tali mezzi forniscono nei processi di diagnosi e cura soprattutto dei pazienti cronici, per i quali, continuità assistenziale, monitoraggio domiciliare, telemedicina, sono essenziali[69].

Con riferimento alla funzionalità, caratteristica comune a molti dei documenti sanitari elettronici menzionati è, anzitutto, quella di assolvere lo scopo primario per il quale sono stati creati, e cioè, principalmente, essere strumenti di supporto per il personale sanitario coinvolto nella cura del paziente.

È, altresì, importante notare che, in tutti gli esempi indicati, alla funzione prettamente clinica, sono di frequente associati ulteriori usi, correlati, seppur distinti: trattasi dell'utilizzo dei dati sanitari per ragioni medico-legali, di "*quality management*", di formazione ed aggiornamento professionale, di ricerca e sanità pubblica etc. Le ragioni di tale estensione d'uso vanno, tra l'altro, ravvisate nel mutamento di paradigma che coinvolge anche il servizio sanitario, mutamento dovuto al diffondersi ed all'evolversi dei sistemi informativi sanitari[70].

---

[69] Il *Patient Health Record* è, oggi, oggetto di crescente attenzione da parte di molti enti di ricerca ed aziende impegnati nel settore biomedico; numerosi sono in tal senso i progetti intrapresi in tutti i Paesi dell'Unione europea. Anche in letteratura non mancano i contributi su questioni teoriche e pratiche connesse a questo strumento di sanità elettronica; tra gli altri: P. FLATLEY BRENNAN, S. DOWNS, G. CASPER, *Project HealthDesign: Rethinking the power and potential of personal health records*, Journal of Biomedical Informatics, Vol. 43, Issue 5, Supplement, 2010, pp. S3-S5; F. UECKERT, M. GOERZ, M. ATAIAN, S. TESSMANN, H. PROKOSCH, *Empowerment of patients and communication with health care professionals through an electronic health record*, International Journal of Medical Informatics, Vol. 70, Issues 2–3, 2003, pp. 99-108; D. F. SITTIG, *Personal health records on the internet: a snapshot of the pioneers at the end of the 20th Century*, International Journal of Medical Informatics, Vol. 65, Issue 1, 2002, pp. 1-6. Sul mutamento degli scenari attuali anche sul fronte medico a seguito della diffusion delle nuove tecnologie, tra gli altri: WORLD HEALTH ORGANIZATION, *mHealth: New Horizons for Health through Mobile Technologies*, Global Observatory for eHealth Services, Vol. 3, 2011; C. HAWN, *Take Two Aspirin and Tweet Me in the Morning: How Twitter, Facebook, and Other Social Media are Reshaping Healthcare*, Health Affairs, 28 (2) 2009: 361-365.

[70] Nell'era moderna il cittadino/paziente è essenzialmente cosmopolita, tende alla mobilità nazionale ed internazionale, necessita pertanto di adeguati strumenti che gli permettano di avere sempre con sé la propria storia clinica, accessibile in qualsiasi momento dal personale autorizzato e facilmente consultabile. Se è vero quanto asserito, è altrettanto vero che in modo crescente le informazioni cliniche non costituiscono più soltanto una proprietà esclusiva del medico e/o della struttura sanitaria che le ha generate, bensì, sempre più

Interrogativo principale rimane, dunque, la definizione di Fascicolo Sanitario Elettronico[71]. In generale, il termine indica una raccolta digitale di dati medici, sanitari e diagnostici, finalizzata ad assicurare l'integrità delle cure del paziente. Per questa ragione occorre che il FSE sia quanto più possibile completo ed al tempo stesso dotato di misure di sicurezza volte a tutelare la riservatezza delle informazioni trattate[72]. Sebbene tale descrizione sia piuttosto generica e priva di riferimenti architetturali o infrastrutturali specifici, al tempo stesso essa individua le caratteristiche salienti ed i relativi profili, tecnici e giuridici, cruciali per l'implementazione dello strumento in esame, tra cui, appunto, la storia clinica del paziente[73], la natura "sensibile" dei dati collezionati in formato digitale, l'esclusività nell'accesso alle informazioni ed i conseguenti profili di responsabilità, civile e penale, per i soggetti non autorizzati al trattamento[74].

---

frequentemente, occorre che esse siano messe a disposizione all'interno del dominio aziendale nel quale sono state formate e, ove richiesto, anche a livello sovra-aziendale e sovranazionale. Queste evidenze sociologiche hanno orientato e continuano ad orientare la tecnologia applicata al dominio sanitario che, tra le altre innovazioni, ha elaborato nuovi mezzi in grado di soddisfare le esigenze di pazienti e personale (sanitario, para-sanitario, amministrativo) coinvolti nei processi di diagnosi e cura. A seguito dell'avvento imperante dei *mobile device* (*laptop, tablet PC, mobile phone, smart phone, media player* etc.) e delle relative applicazioni il consumatore riveste un ruolo sempre più centrale nella "gestione" della propria salute: non più soltanto beneficiario di cure ma stratega del proprio percorso di salute.
L'utilizzo dei *mobile devices* nel settore sanitario sono crescenti; la recente diffusione di tali strumenti ha aperto un vivace dibattito, tra gli studiosi, sull'implementazioni tecniche da adottare nonché, tra i giuristi, sui profili di legittimità e sulle forme di responsabilità ad essi collegati. Per approfondimenti, si rinvia tra gli altri a: H. KHARRAZI, R. CHISHOLM, D. VANNASDALE, B. THOMPSON, *Mobile personal health records: An evaluation of features and functionality Review Article*, International Journal of Medical Informatics, Vol. 81, Issue 9, 2012, pp. 579-593; PAUL C. TANG, JOAN S. ASH, DAVID W. BATES, J. MARC OVERHAGE, DANIEL Z. SANDS, *Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption*, Journal of the American Medical Informatics Association, Vol. 13, Issue 2, 2006, pp. 121-126.

[71] Puntuali definizioni si trovano anche in D. GARETS, M. DAVIS, *Electronic Patient Records. EMRs and EHRs*, Healthcare Informatics, 2005.

[72] *Cfr*. I. IAKOVIDIS, *Towards Personal Health Record: Current situation, obstacles and trends in implementation of Electronic Healthcare Records in Europe*, International Journal of Medical Informatics, n. 52, 128, 1998, pp. 105-117.

[73] Analogamente a quanto avviene per le cartelle sanitarie cartacee, la tipologia di informazioni sanitarie è piuttosto diversificata. Sintetico, ma efficace, è in proposito quanto chiarito da Eichelberg et at.: "*Operational EHRs include information such as observations, laboratory tests, diagnostic imaging reports, treatments, therapies, drugs prescribed, dispensed and administered, patient identifying information and demographics, legal permissions, allergies and the identities of healthcare professionals and provider organisations who have provided healthcare. This information is stored in various electronic formats using a multitude of medical information systems available on the market*" (in M. EICHELBERG et al., *Electronic Health Record Standards - a brief overview, conference paper for Information Processing in the Service of Mankind and Health*, ITI 4th International Conference on Information and Communications Technology, 2006).

[74] Pur suggerendo elementi interessanti per l'analisi, la definizione di EHR proposta da "*Health Information Managment System Society*" (HIMSS), organizzazione specializzata nel settore nell'*e-Health*, discosta da quella ivi proposta essenzialmente sull'elemento della completezza delle informazioni clinico-sanitarie: più che la "storia clinica del paziente", il FSE longitudinale conserva i dati inerenti ad una singola attività specialistica. La definizione di HIMSS è disponibile alla pagina http://www.himss.org/ASP/topics_ehr.asp.

2. IL SISTEMA INFORMATIVO SANITARIO: BREVI CENNI

Il contesto del quale il Fascicolo Sanitario Elettronico fa parte, contesto senza il quale non sarebbero possibili la sua realizzazione e, soprattutto, la sua implementazione, è il sistema informativo sanitario. Molti sono, a tutt'oggi, i fattori di complessità dei sistemi nazionali, spesso conseguenza della pluralità di attori (operatori e strutture) coinvolti; a titolo esemplificativo, di seguito si riportano alcuni casi osservabili a livello locale, pur consapevoli che le compagini territoriali, nazionali e transnazionali, sono di gran lunga più articolate.

I processi aziendali appaiono per loro natura poliedrici: tutte le componenti dell'organigramma, dalla direzione agli operatori sanitari sono, infatti, portatrici di interessi differenti e, seppur per motivi diversi, tutti i soggetti coinvolti nell'*iter* assistenziale quotidianamente necessitano di accedere alle informazioni conservate nei fascicoli sanitari elettronici. Se, da una parte, gli uffici amministrativi bisognano dei dati identificativi del paziente (anagrafica, previdenza, assicurazione sanitaria etc.) per gestire servizi e costi connessi alle prestazioni erogate, dall'altra, gli operatori sanitari (medici, infermieri, tecnici di laboratorio etc.), ciascuno per le proprie competenze e specializzazioni, sono al tempo stesso produttori e fruitori delle informazioni sanitarie che compongono il quadro clinico dell'assistito (*cfr. fig. 3*).

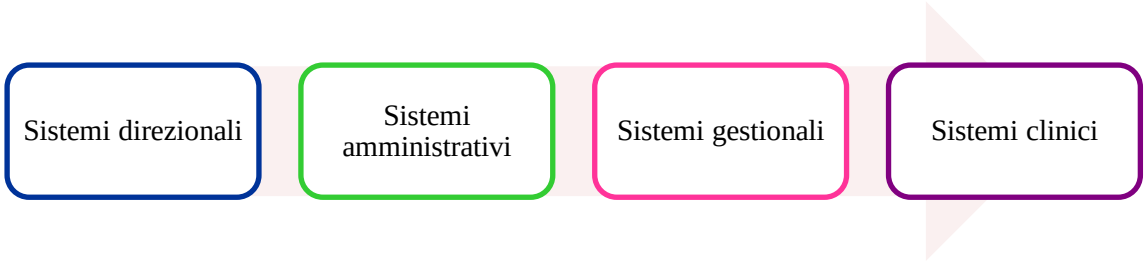


Figura 3 - Esemplificazione di un processo aziendale sanitario

Altrettanto significativa è, poi, la varietà organizzativa adottata, ad esempio, all'interno dei reparti ospedalieri; sovente, infatti, le realtà che operano nella medesima azienda sanitaria, pubblica o privata, si strutturano secondo sistemi di gestione non affini tra loro[75].

Anche dal punto di vista delle infrastrutture dei sistemi informativi, l'eterogeneità - locale, nazionale, transnazionale - non giova al raggiungimento di buoni livelli di funzionalità ed interoperabilità, raggiungibili, soprattutto, attraverso l'automazione delle transazioni tra

[75] La riflessione sugli aspetti organizzativi dei sistemi sanitari è da tempo oggetto del dibattito tra *managers* ed esperti; di interesse, tra gli altri, O. GRÜN, *Taming Giant Projects. Management of Multi-Organization Enterprises*, Berlin, Springer, 2004, pp. 271.

operatori e strutture sanitarie. Questo risultato rappresenta, al contrario, l'*optimum* per un'efficace implementazione del Fascicolo Sanitario Elettronico.

Lo scenario illustrato richiede, pertanto, che l'organizzazione dei sistemi informativi sanitari, di cui fanno parte attori, attività, infrastrutture e servizi, sia ben strutturata, e, alla luce delle nuove tecnologie, modernizzata[76].

Secondo quanto previsto dallo *standard* "CEN/TC251 EN ISO 12967-1:2011"[77], elementi costitutivi dei sistemi informativi sanitari sono, anzitutto, i servizi, come di seguito qualificati: (i) "clinici", ai quali è affidato il trattamento di dati del cittadino (Centri Unici Prenotazioni, monitoraggio domiciliare, telemedicina etc.); (ii) "di informazione sanitaria", preposti al trattamento delle conoscenze sanitarie (ad esempio, sorveglianza epidemiologica, monitoraggio della qualità dell'assistenza, informazioni cliniche per il pubblico); (iii) "amministrativi", competenti per il trattamento dati sulle strutture (rimborsi prestazioni e *budget* medico, *datawarehouse* per *manager* sanitari e così via).

Analogamente a quanto accade in ogni meccanismo di comunicazione (scritta, orale, paraverbale e digitale), in cui, perché il messaggio sia correttamente trasmesso, è essenziale la coesistenza di alcune componenti, quali emittente, canale comunicativo, referente, informazione, codice formale per significare l'informazione, ricevente, anche per l'operabilità dei fascicoli sanitari elettronici è indispensabile la progettazione di reti di trasmissione adeguate. Anelli infrastrutturali essenziali, distinti ma al tempo stesso complementari, di un sistema informativo sanitario sono quello tecnologico, informativo e della conoscenza (sinteticamente rappresentati in *figura 4*).

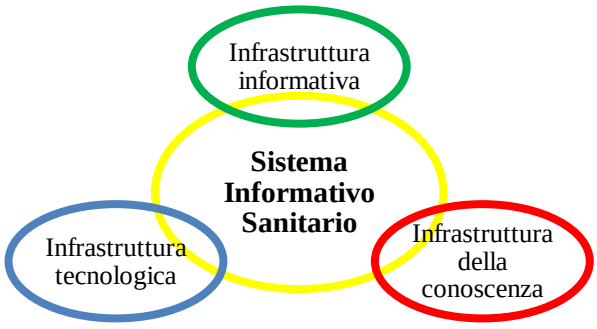


Figura 4 - Infrastrutture di un Sistema Informativo Sanitario

[76] Pluridecennali sono le ricerche, teoriche ed applicate, su questo tema, ricerche che hanno portato ad iniziative progettuali, comunitarie e nazionali, concrete ed i cui riscontri positivi, come si dirà, non sono tardati ad arrivare. Per approfondimenti: A. ROSSI MORI, F. CONSORTI, R. NARDI, F. L. RICCI (a cura di), *Un quadro di riferimento sulle tecnologie dell'informazione nel settore sanitario*, Consiglio Nazionale delle Ricerche - Istituto Tecnologie Biomediche, 2003, pp. 64.

[77] EUROPEAN COMMITEE FOR STANDARDIZATION (CEN), TECHNICAL COMMITEE 251, *EN ISO 12967-1:2011*, "*Health informatics - Service architecture - Part 1: Enterprise viewpoint*" (ISO 12967-1:2009).

Trasferire conoscenza e, in questo caso, trasferire innovazione, è uno dei principali obiettivi sottesi alla creazione di un sistema informativo: a poco, infatti, varrebbero efficienti impianti tecnologici non in grado di essere utilizzati dai destinatari finali. Il coinvolgimento delle reti politica e legislativa, la predisposizione di adeguati percorsi formativi per gli utenti, l'introduzione di nuovi paradigmi culturali orientati alla sanità elettronica, sono solo esempi delle modalità con cui l'infrastruttura della conoscenza può di fatto operare.

Asse portante di un sistema informativo sanitario è, poi, l'infrastruttura tecnologica, attraverso la quale i processi clinico-decisionali possono essere centralizzati. Affinché tale risultato sia in pratica raggiungibile, è, tuttavia, necessario costituire ed implementare una serie di componenti, come banda larga, reti *intranet* aziendali, firme elettroniche, documenti personali dotati di *chip* elettronici per la memorizzazione di informazioni sanitarie.

Cuore dell'infrastruttura informativa è la predisposizione di piattaforme sanitarie informative integrate, basate su modelli di dati ed interfacce di accesso standardizzati[78], utilizzabili nelle transazioni elettroniche ed accessibili al pubblico dominio. Registri di metadati per la rappresentazione uniforme dei *dataset* di interesse pubblico, modelli concettuali condivisi, sistemi di codifica possono migliorare l'armonizzazione delle suddette transazioni.

Favorire l'interoperabilità dei fascicoli sanitari elettronici grazie all'utilizzo di *standard* è un obiettivo elevato, ma, al tempo stesso, è indispensabile da pianificare e, verosimilmente, da raggiungere[79]. A tal fine, occorre che tutti i soggetti coinvolti nei processi di diagnosi e cura convergano verso prassi sempre più uniformi, definendo quali vocabolari clinici[80] o ontologie adottare, le tecniche di cui avvalersi per lo scambio dei documenti sanitari, le interfacce grafiche da utilizzare, le modalità con cui attribuire gli

[78] *Cfr.*, ad esempio, EN ISO 12967-1:2011 "*Health informatics - Service architecture - Part 1: Enterprise viewpoint*" (ISO 12967-1:2009), CEN/TC 251 - EN 13606-2:2007, "*Health informatics - Electronic health record communication - Part 2: Archetypes interchange specification*" e HL7, "*Clinical Document Architecture*", *Release 2*. Analogamente all'attività svolta a livello europeo da CEN/TC251, a livello internazionale una vasta opera di standardizzazione in informatica sanitaria è compiuta da *Health Level 7*. La collaborazione ventennale delle due organizzazioni ha, peraltro, introdotto una vera e propria nuova generazione di *standards* testati sul campo.

[79] In proposito di interesse lo studio EMPIRICA, *ICT standards in the health sector: current situation and prospects*, Final report, v. 3.0, Special Study n. 1, 2008, pp. 84 e D. KARLA, *Electronic Health Records Standards*, IMIA Year Book of Medical Informatics, 2006, pp. 136-144.

[80] Come, ad esempio SNOMED-CT, LOINC, ICD, HL7.

identificativi dei pazienti, le regole da seguire per la gestione della *privacy* e della sicurezza e così via[81].

Tali risultati, hanno, peraltro, un'importante conseguenza: disegnare uno strumento digitale funzionale ad accompagnare il paziente lungo tutto l'*iter* delle cure, sia nella medesima struttura assistenziale sia, in modo trasversale, in più contesti di cura appartenenti ad una determinata realtà territoriale o, in altre circostanze, a realtà diverse, di carattere nazionale o sovranazionale[82]. Le tre componenti descritte rappresentano, quindi, il contesto all'interno del quale un Fascicolo Sanitario Elettronico può essere positivamente sviluppato. Ancora una volta è bene sottolineare che, seguendo un approccio olistico, il vero beneficiario di un sistema efficiente è soltanto il cittadino, attorno al quale la frammentazione delle informazioni concernenti la sua "storia clinica" può trovare unità[83] (*cfr. fig. 5*).

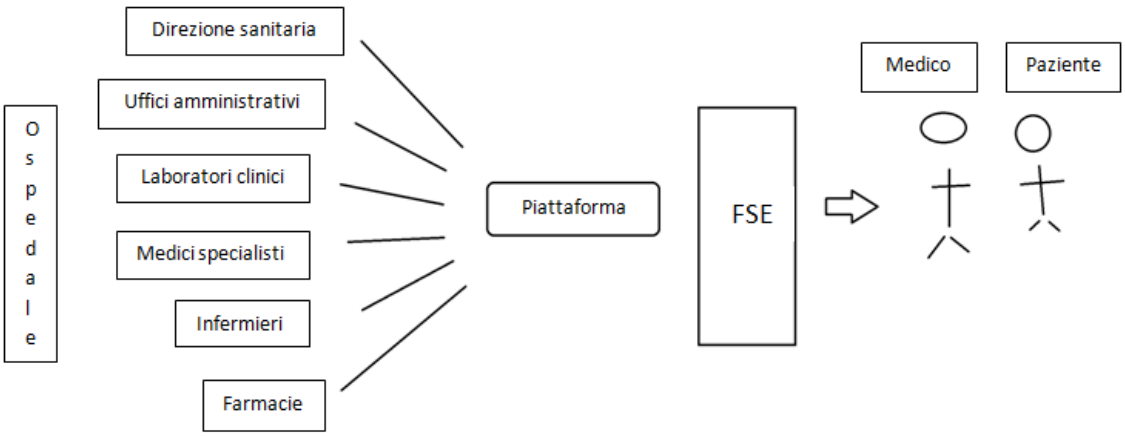


Figura 5 - Integrazione olistica delle informazioni sanitarie, *patient-based*

[81] Ne verrà dato conto nel corso del capitolo, ma in generale può qui osservarsi che per gestire i problemi di interoperabilità dei fascicoli sanitari elettronici sono attualmente disponibili *standards* elaborati da diverse organizzazione, come "*Health Level 7*", "*European Committe for Standardization*", "*International Organization for Standardization*", "*OpenEHR*", "*Integrating the Healthcare Enterprise*".

[82] Per quanto concerne la letteratura italiana sui temi della sanità elettronica e del Fascicolo Sanitario Elettronico un tentativo di sistematizzazione delle diverse forme di documenti sanitari digitali è proposto in M. MORUZZI, *e-Health e Fascicolo Sanitario Elettronico*, Il Sole 24 Ore, 2009, pp. 364. Nell'evidenziare gli elementi caratteristici e distintivi delle varie forme di documenti sanitari digitali, l'Autore pone una particolare attenzione sugli aspetti architetturali dei singoli strumenti, aspetti che, spesso, sono legati in modo specifico alle diverse funzionalità proprie di ciascun tipo di documento. Ad esempio, la rete verticale su cui si basa *Electronic Medical Record* favorisce l'organizzazione dell'azienda sanitaria, mentre la rete orizzontale in cui è configurabile *Electronic Health Record* meglio si adatta al "governo della continuità della cura tra ospedale e territorio".

[83] Di interesse, per comprendere ulteriormente il complesso scenario finora descritto e l'importanza di promuovere sistemi integrati: NATIONAL INSTITUTES OF HEALTH - NATIONAL CENTER FOR RESEARCH RESOURCES, *Electronic Health Record Overview*, MITRE Center for Enterprise, McLean, Virginia, 2006, pp. 30.

Distinte dalle componenti infrastrutturali, ma ad esse funzionali, sono le *policy*, fondamentali per la sicurezza e la produttività dell'organizzazione aziendale e, con specifico riferimento ai temi della presente ricerca, per la definizione dei principi riguardanti il trattamento dei dati dell'assistito (modalità di rilascio del consenso, regolamentazione dell'accesso ai dati sanitari, tutela del diritto alla riservatezza e del diritto all'oblio etc.).

3. IL PROCESSO DI STANDARDIZZAZIONE IN SANITÀ

Come già evidenziato, affinché tutti i summenzionati obiettivi siano raggiungibili, e, quindi, siano realizzabili strumenti digitali tra loro compatibili ed interoperabili, è indispensabile l'adozione di norme tecniche condivise. Analogamente a quanto avviene, ad esempio, nel campo delle telecomunicazioni o dell'informatica giuridica, anche l'informatica sanitaria ha sviluppato, ormai da diversi decenni, molteplici *standard* operativi[84].

Principali organizzazioni di standardizzazione nel settore sanitario sono: "*International Standardization Organization*" (ISO), "*European Committe for Standardization*" (CEN), "*Health Level 7*" (HL7), "*National Electrical Manufacturers Association*" (NEMA), "*International Health Terminology Standards Development Organization*" (IHTSDO), "*openEHR*", "*Integrating the Healthcare Enterprise*" (IHE). Altrettanto efficaci le iniziative di standardizzazione intraprese in questo ambito da "*World Health Organization*" (WHO), "*Institute of Electrical and Electronics Engineers*" (IEEE), "*Regenstrief Institute Inc.*", "*Continua Health Alliance*" (Continua)[85]. Di seguito si riportano annotazioni di carattere generale relative alle summenzionate organizzazioni, sottolineando, in particolare, i profili attinenti alle tematiche oggetto della ricerca. Per una descrizione più analitica di alcuni degli *standard* sanitari maggiormente utilizzati nella prassi, si rinvia alla presentazione dei selezionati progetti europei e nazionali; nel presente

[84] A seconda della loro provenienza, si distinguono *standard* (o norme) volontari, *de facto* o imposti dalle autorità. Tra gli altri, si rinvia al *deliverable* Q-REC, WP3, *Inventory of Relevant Standards for EHR Systems*, v. 0.8, 2007, pp. 95, particolarmente significativo per la panoramica fornita sugli *standards* utilizzati, in modo diretto o indiretto, nel contesto del Fascicolo Sanitario Elettronico, quali, ad esempio, "*architecture standard*", "*modelling standard*", "*terminology standard*", "*ontology standard*", "*classification system and standard*", "*identifier and ID management standard*", "*standard for communication security*", "*standard for application security*", "*privacy standard*", "*standard for infrastructural services*", "*communication protocol standard*", "*standard for formal languages*", "*development process standard*" etc.

[85] Per approfondimenti si rinvia ai siti *web* ufficiali delle organizzazioni citate, disponibili agli indirizzi: http://www.iso.org/, http://www.cen.eu/, http://www.hl7.org/, http://medical.nema.org/, http://www.ihtsdo.org/, http://www.openehr.org/, http://www.ihe.net/, http://www.who.int/, https://www.ieee.org/, http://loinc.org/, http://www.continuaalliance.org/.

studio, si è, infatti, preferito adottare un approccio *bottom-up*, evitando, pertanto, di proporre una rassegna, fine a se stessa, degli *standard* esistenti.

"*International Organization for Standardization*" è la più importante organizzazione mondiale per la definizione di norme tecniche. Fondata nel 1947, fin da allora essa ha prodotto più di 19.500 norme internazionali dedicate a diversi settori, dall'alimentare alla sicurezza informatica, dall'agricoltura al *business*, fino alla salute. Diverse sono le Commissioni Tecniche in cui è organizzata ISO, ad oggi, precisamente, duecentosettantotto; per quanto concerne gli *standard* informatico-sanitari, essi sono sviluppati dalla Commissione Tecnica 215, a sua volta articolata in sotto-commissioni[86]. Scopi principali della Commissione "*Health Informatics*" sono la promozione dell'interoperabilità tra sistemi indipendenti, il miglioramento della compatibilità tra dati ed informazioni sanitarie nonché la riduzione delle ridondanze[87].

"*European Committe for Standardization*" è l'ente europeo competente per l'armonizzazione e la standardizzazione di norme tecniche. Fondato nel 1975, è l'unica organizzazione europea riconosciuta dalla Direttiva 98/34/CE per la pianificazione, la stesura e l'adozione di norme europee in tutti i settori di attività economica, ad eccezione di quello elettrotecnico e delle telecomunicazioni[88]. Analogamente a "*International Standardization Organization*", anche l'attività di standardizzazione informatico-sanitaria di CEN è operata da una Commissione Tecnica, la 251, a sua volta organizzata in *Working Group*[89]. La maggior parte delle norme prodotte da CEN/TC 251 riguardano i profili della rappresentazione delle informazioni, la standardizzazione dei messaggi, i fascicoli sanitari elettronici[90]. Incarico altrettanto rilevante, affidato, nel 2006, dalla Commissione europea a "*European Committe for Standardization*", è l'implementazione dell'interoperabilità in sanità[91].

---

[86] Attualmente le sotto-commissioni ed i *Working Group* operanti sono: TC 215/CAG 1 "*Executive council, harmonization and operations*", TC 215/WG 1 "*Data structure*", TC 215/WG 2 "*Data interchange*", TC 215/WG 3 "*Semantic content*", TC 215/WG 4 "*Security*", TC 215/WG 6 "*Pharmacy and medicines business*", TC 215/JWG 7 "*Joint ISO/TC 215 - IEC/SC 62A WG: Application of risk management to information technology (IT) networks incorporating medical devices*", TC 215/WG 9 "*SDO Harmonization*".

[87] *Cfr*. "Appendice".

[88] *Direttiva 98/34/CE del Parlamento europeo e del Consiglio del 22 giugno 1998 che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione*, pubblicata in G.U. n. L 204 del 21.7.1998.

[89] Sotto-commissioni ad oggi esistenti sono: CEN/TC 251/WG 1 "*Information models*", CEN/TC 251/WG 2 "*Terminology and knowledge representation*", CEN/TC 251/WG 3 "*Security, Safety and quality*", CEN/TC 251/WG 4 "*Technology for interoperability*".

[90] *Cfr*. "Appendice".

[91] EUROPEAN COMMISSION, *M/403 Mandate to the European Standardisation Organisations CEN, CENCELEC and ETSI in the Field of Information and Communication Technologies, Applied to the Domain of eHealth*, December 2006.

L'impegno di HL7, organizzazione fondata nel 1987 ed accreditata presso "*American National Standards Institute*", è prevalentemente dedicato allo sviluppo di *standard* nell'IT sanitario. Come ISO e CEN, "*Health Level 7*" è organizzata in *Technical Committee* e *Special Interest Group*, ciascuno competente in specifiche aree[92]. Scopo principale di HL7 è definire un *framework* per lo scambio, l'integrazione, la condivisione ed il recupero delle informazioni sanitarie elettroniche tra sistemi informativi sanitari[93].

"*U.S. National Electrical Manufacturers Association*", fondata nel 1926, è l'ente responsabile dello sviluppo di *standard* per immagini mediche "*Digital Imaging and Communications in Medicine*" (DICOM). Principali compiti di NEMA sono la definizione di protocolli di rete per la standardizzazione delle comunicazioni tra dispositivi aderenti agli *standard* DICOM, la determinazione di informazioni - sintattiche e semantiche - necessarie per lo scambio di immagini mediche, la descrizione di specifiche dei supporti di memorizzazione e di formati di *file* per le immagini medicali.

L'implementazione di "*Systematized Nomenclature Of Medicine Clinical Terms*" (SNOMED CT), il più vasto *thesaurus* multilingue di termini clinici con una fondazione ontologica, è curato da "*International Health Terminology Standards Development Organization*". SNOMED CT fornisce la principale terminologia generale da utilizzare nel Fascicolo Sanitario Elettronico; contiene, infatti, più di 311.000 concetti attivi, in continuo aumento, con significati unici e definizioni "*logic-based*" organizzate in gerarchie con livelli multipli di granularità.

"*OpenEHR*" è una comunità virtuale impegnata sui temi dell'interoperabilità e computabilità in materia di sanità elettronica. In particolare, "*OpenEHR*" implementa uno *standard* "aperto" per la gestione, il recupero e lo scambio di dati sanitari, mostrando preciso interesse per il Fascicolo Sanitario Elettronico. La Fondazione "*OpenEHR*" ha predisposto specifiche che definiscono un modello di informazione sanitaria, un linguaggio per la "costruzione di modelli clinici" ed un linguaggio di *query*. In *OpenEHR*, componenti

[92] Ne sono esempi: "*Electronic Health Record*", "*Clinical Decision Support*", "*Security*", "*Patient Care*", "*Structured Document*", "*Pharmacy*", "*Regulated Clinical Research Information Management*", "*Clinical Interoperability Council*", "*Public Health and Emergency Response*".

[93] Gli *standard* HL7 sono raggruppati in sette categorie di riferimento: (i) "campioni primari", *standard* per integrazioni di sistema, interoperabilità e la conformità; (ii) "norme fondamentali", definiscono gli strumenti fondamentali per la costruzione delle norme e l'infrastruttura tecnologica sottesa; (iii) "domini clinici e amministrativi", messaggistica e *standard* specialistici; (iv) "profili di EHR", tali norme forniscono modelli funzionali per la gestione di fascicoli sanitari elettronici; (v) "guida di attuazione", raccoglie guide di implementazione e/o documenti di supporto creati per essere utilizzato in combinazione con gli *standard* esistenti; (vi) "regole e referenze", specifiche tecniche, strutture di programmazione e linee guida per lo sviluppo di *software* e *standard*; (vii) "educazione e consapevolezza", in cui sono disponibili "*HL7's Draft Standards for Trial Use*" e progetti in corso, nonché altre risorse utili e strumenti per la comprensione e l'adozione di *standard* HL7.

e sistemi sono "aperti", in termini di dati (*cfr*. "*openEHR XML Schema*"[94]), modelli (questi seguono "*the openEHR Archetype Model - Archetype Definition Language*"[95]) ed interfacce di programmazione delle applicazioni (*API*).

L'iniziativa "*Integrating the Healthcare Enterprise*", nata negli Stati Uniti nel 1998 ad opera di "*Radiological Society of North America*" e "*Healthcare Information and Management Systems Society*", si propone di chiarire in che modo i sistemi informativi sanitari debbano utilizzare gli *standard* esistenti (in particolare, *DICOM* e *HL7*) per renderli realmente integrabili. IHE non definisce un vero e proprio *standard* di comunicazione, bensì, costruisce un linguaggio univoco, eliminando le possibili ambiguità tra gli *standard* adottati. A tal fine, "*Integrating the Healthcare Enterprise*" coinvolge produttori ed utenti dei sistemi informativi sanitari per identificare e risolvere i problemi d'interoperabilità; per l'implementazione dei profili delineati sono redatti "*Technical Framework*", specifici per le diverse aree coinvolte[96].

Nella presentazione delle principali iniziative sul fronte della standardizzazione medico-sanitaria, altresì rilevante richiamare quella intrapresa, fin dal 1994, dall'Organizzazione Mondiale alla Sanità: trattasi dello *standard* "*International Classification of Diseases*" (ICD), approvato nel 1990 durante la 43^{esima} assemblea mondiale della sanità. ICD, attualmente alla decima revisione (ICD-10), raccoglie una classificazione internazionale delle malattie ed altri problemi ad esse correlati, particolarmente utile per studi statistici ed epidemiologici, nonché per la gestione di quesiti inerenti salute ed igiene pubblica[97].

Altrettanto efficaci le azioni intraprese in questo settore da "*Institute of Electrical and Electronics Engineers*", associazione professionale fondata nel 1963, la cui attività è prevalentemente dedicata allo studio della trasmissione di segnali ed alla gestione delle apparecchiature. È, oggi, una delle principali organizzazioni impegnate nello sviluppo di *standard* industriali che coprono vari campi, quali l'energia elettrica, le tecnologie biomediche e l'assistenza sanitaria, la tecnologia dell'informazione, la sicurezza delle informazioni e delle telecomunicazioni, l'elettronica di consumo, i trasporti, le

---

[94] Per approfondimenti si rinvia alla *homepage* di "*OpenEHR*" (consulanile all'indirizzo http://www.openehr.org/) e, in particolare, alla sezione del sito dedicata agli *standard*.
[95] *Ibidem*.
[96] Settori nei quali sono redatti ed aggiornati i "*Technical Framework*" di IHE sono: "*Anatomic Pathology*", "*Cardiology*", "*Eye Care*", "*IT Infrastructure*", "*Laboratory*", "*Patient Care Coordination*", "*Patient Care Device*", "*Pharmacy*", "*Quality, Research and Public Health*", "*Radiation Oncology*", "*Radiology*".
[97] Per approfondimenti sullo standards, si rinvia alla pagina ufficiale del sito dell'OMS ad esso dedicata, consultabile all'indirizzo http://www.who.int/classifications/icd/en/.

nanotecnologie. Tra i prodotti sviluppati da IEEE per l'interoperabilità sanitaria si ricorda la famiglia di *standard* ISO/IEEE 11073[98].

"LOINC®", approvato da "*Clinical Laboratory Association* e *College of American Pathologists*", ha preso avvio nel 1994 ad opera di "*Regenstrief Institute Inc.*", organizzazione *no-profit* americana dedicata alla ricerca medica. Il *database*, contenente una vera e propria nomenclatura per dati di laboratorio e misure sui segnali, è, appunto, articolato in due parti, quella dedicata al laboratorio in cui sono reperibili le categorie più diffuse, come chimica, ematologia, sierologia, microbiologia, tossicologia; la parte clinica include, invece, voci per segni vitali, emodinamica, ECG, procedure gastro-endoscopiche etc. "LOINC®" facilita lo scambio e la condivisione dei risultati per la cura clinica, la gestione dei risultati, e la ricerca.

Nel settore della standardizzazione medico-sanitaria parimenti importante è il ruolo svolto da "*Continua Health Alliance*", organizzazione *no-profit* alla quale aderiscono più di duecento aziende di tutto il mondo. Di interesse per questo studio sottolineare l'impegno innovativo di "*Continua Health Alliance*" nella definizione di *standard* industriali e tecnologie di sicurezza per sistemi connessi come *smartphone*, *gateway* e dispositivi di monitoraggio remoto; in tal senso, particolarmente centrale è l'attività condotta per l'interoperabilità di *Personal Health System*. Scopo principale dell'organizzazione è quello di sviluppare un sistema per fornire assistenza sanitaria personalizzata; settori nei quali *Continua* investe con maggiore interesse sono quello relativo alla gestione delle malattie croniche, all'invecchiamento, alla salute e forma fisica[99].

4. ANALISI DI SELEZIONATI PROGETTI EUROPEI E NAZIONALI

Il presente paragrafo è dedicato alla presentazione di selezionati progetti, europei e nazionali, in tema di Fascicolo Sanitario Elettronico.

Esaminati i progetti in essere tra i 27 Paesi membri dell'Unione, la ricerca ha tenuto conto di esperienze pilota in essere a livello europeo, dei contesti con avanzate e solide radici nel settore dell'*e-Health* (come nel caso dei Paesi scandinavi), di azioni di più recente evoluzione tecnica e giuridica in materia di FSE nonché, infine, dello scenario italiano.

[98] *Cfr*. "Appendice".

[99] Similmente a quanto già osservato per alcune delle organizzazioni citate, anche *Continua Health Alliance* svolge la sua attività attraverso *Working Group*; quelli al momento operanti sono i seguenti: "*Marketing Council*", "*Global Development & Outreach*", "*European Union*", "*US Policy*", "*Technical*", "*Use Case*", "*Market Adoption*", "*Regulatory*", "*Test & Certification*".

In particolare, per quanto concerne il panorama comunitario, esclusiva attenzione è stata rivolta al progetto "*Smart Open Services for European Patients*" (*epSOS*); per quanto, invece, riguarda lo scenario nazionale, lo studio riferisce di alcune tra le iniziative più significative intraprese nei seguenti Paesi membri dell'UE: Austria, Danimarca, Italia[100].

Scopi principali dell'analisi sono, da una parte, ricavare gli elementi architetturali del Fascicolo Sanitario Elettronico, dall'altra presentare l'effettivo stato dell'arte ed i livelli di interoperabilità (organizzativa, tecnica e semantica) attualmente esistenti, a partire dal campione di progetti selezionati.

4.1 UNIONE EUROPEA

Nel capitolo dedicato alla azioni politiche e legislative intraprese dalla Commissione europea per l'introduzione delle Tecnologie dell'Informazione e della Comunicazione in sanità, particolare attenzione è stata rivolta al documento "*eHealth Action Plan*", vero e proprio motore per la creazione di uno spazio europeo rivolto alla sanità elettronica. A livello transazionale, il monito della Commissione si è, tra l'altro, concretizzato in un'importante iniziativa, il progetto "*Smart Open Services for European Patients*".

4.1.1 PROGETTO "*EPSOS*"

"Smart Open Services For European Patients - epSOS" è un progetto pilota co-finanziato, per il periodo luglio 2008 - dicembre 2013, dalla Commissione europea ("Programma Competitività e Innovazione dell'UE 2007-2013", ICT-PSP, call 1-2007)[101]. È il primo, ad oggi, per numero di Paesi coinvolti; riunisce, infatti, ventitrè Stati, rappresentati da pubbliche amministrazioni, centri di competenza nazionali ed imprese[102].

Obiettivo di *epSOS* è assicurare l'interoperabilità tra analoghe iniziative nazionali, per consentire ai professionisti sanitari l'accesso ai dati di un paziente, utilizzando la propria

[100] Un contributo importante per la ricognizione dello stato dell'arte europeo su progetti nazionali in materia di Fascicolo Sanitario Elettronico è lo studio, condotto nel triennio 2006-2009, A. K. STROETMANN, R. HAMMERSCHMIDT, V. N. STROETMANN, I. MOLDENAERS, *eHealth in Action. Good Practice in European Countries. Good eHealth Report*, Luxemburg, 2009, pp. 60, in cui è presentato lo stato dell'arte in materia di *e-Health* e FSE di 30 Paesi del continente europeo (Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, United Kingdom). Altrettanto significativo nell'affrontare la medesima tematica è poi il più recente studio A. K. STROETMANN, J. ARTMANN, V. N. STROETMANN, WITH D. PROTTI, J. DUMORTIER, S. GIEST, U. WALOSSEK, D. WHITEHOUSE, *European countries on their journey towards national eHealth infrastructures. eHealth Strategies Report*, 2011, pp. 61.

[101] La *homepage* del Progetto pilota è consultabile all'indirizzo http://www.epSOS.eu/; nella sezione del sito "*download - deliverables*" sono disponibili i documenti di lavoro di *epSOS*.

[102] *Cfr*. "Appendice".

lingua madre ed avvalendosi di tecnologie e sistemi informativi già in essere. L'ambiente operativo nel quale, dunque, si sviluppa il Progetto pilota è caratterizzato da una forte eterogeneità: a livello nazionale, infatti, molteplici e diversificati sono gli obiettivi politici fissati, le strategie di *business* intraprese, le procedure amministrative adottate, i sistemi informativi sanitari disegnati, le tecnologie adoperate. La suddetta eterogeneità non costituisce, tuttavia, un punto di debolezza o criticità nella realizzazione di *epSOS*, bensì, un elemento strutturale tenuto presente nell'attuazione delle varie fasi progettuali[103]. Ed infatti, un pilastro fondante del sistema informativo europeo è ottenere la massima integrazione con lo stato dell'arte esistente per ciò che concerne sia i profili legislativi sia quelli infrastrutturali; esclusivamente ove necessario - secondo quanto reso noto dai redattori del Progetto - saranno apportate modifiche a quanto già realizzato a livello territoriale, e, comunque, al solo scopo di garantire i risultati auspicati.
Rientra in questa visione un altro aspetto: i dati dell'assistito possono essere scambiati tra i sistemi informativi sanitari, rimanendo, però, nella gestione, e dunque nella responsabilità giuridica, dell'ente sanitario emittente; a titolo esemplificativo, qualsiasi utente *epSOS* autorizzato - qui inteso come operatore sanitario, identificato in modo univoco con un proprio ID - può accedere alle informazioni di "*Patient Summary*" e/o "*ePrescription*" "in sola modalità di lettura", senza, cioè, apportare ai documenti consultati alcuna modifica[104]. Principali beneficiari del sistema progettato sono i pazienti, i quali, in linea con quanto auspicato da *epSOS*, potranno godere di prestazioni sanitarie transfrontaliere più efficienti ed efficaci, nel rispetto del principio di riservatezza per ciò che attiene al trattamento dei dati personali.

Mezzo per raggiungere la summenzionata interoperabilità transnazionale è lo sviluppo di un *framework* tecnologico per l'*e-Health* e di un'infrastruttura *IT* che permettano di accedere, in modo sicuro, alle informazioni sanitarie localizzate in altri Paesi, con particolare attenzione, appunto, ai dati registrati in "*Patient Summary*" ed "*ePrescription*". Primario è in *epSOS* il concetto di "*circle of trust*" che richiede un impegno costante e centrale dei Paesi partecipanti per la protezione dei dati personali sanitari; la fiducia appena richiamata è, peraltro, necessaria non soltanto a livello sovranazionale, ma anche

[103] *Cfr.* "*Interoperability definition*" in SMART OPEN SERVICES FOR EUROPEAN PATIENTS, *Open eHealth initiative for a European large scale pilot of Patient Summary and electronic Prescription, D3.3.3 epSOS Interoperability Framework, D3.3.3_v. 2.3*, D3.3.3_v.2.3, 15.04.2010, p. 5.
[104] SMART OPEN SERVICES FOR EUROPEAN PATIENTS, *Open eHealth initiative for a European large scale pilot of Patient Summary and electronic Prescription, D3.3.2 Final epSOS, System Technical Specification, D3.3.2_v1.4*, WP3.3, D3.3.2_v1.4, 28.04.2010, p. 35.

all'interno dei singoli sistemi informativi sanitari nazionali[105]. Attorno al concetto di comunicazione sicura ruota, quindi, l'intera infrastruttura *epSOS*, la quale, ad esempio, a conferma di ogni singola transazione e movimento di dati ("*Query, Retrive and Notify*"[106]), richiede meccanismi di autenticazione reciproca tra richiedente ed emittente, di identificazione (univoca e non ripudiabile)[107], di *audit trail*[108].

Principali dati sanitari oggetto dell'ambiente *epSOS* sono, appunto, quelli contenuti in *Patient Summery* (anagrafica, storia medica dell'assistito - come informazioni sanitarie più importanti e trattamenti in corso -, informazioni sul "*Patient Summary*" - ad esempio, quando e da chi è stato generato il documento -, etc.), "*ePrescription*" (prescrizioni farmaceutiche del paziente, inviate, in modalità digitale, dal medico alle farmacie) ed "*eDispense*" (informazioni relative ai farmaci dispensati dal farmacista, inviate al sistema di gestione del fascicolo sanitario elettronico del paziente).

L'architettura su cui si basa *epSOS* segue il paradigma "*Service Oriented Architecture*", che, nel caso del Progetto in esame, è organizzata sui seguenti livelli: "*Business View*", "*Information System View*" e "*Technology View*". Centrali sono, qui, i ruoli di *service provider*, *service consumer* e *service registry*, ruoli tra loro del tutto autonomi ma, al tempo stesso, complementari.

Affinché le summenzionate azioni per lo scambio di informazioni tra i Paesi ("*Query, Retrive and Notify*") possano essere realizzate, prerequisito fondamentale di ogni sistema nazionale è disporre di un *gateway*, più esattamente un "*National Contact Point*", attraverso il quale effettuare comunicazioni sincrone all'interno di *epSOS*, comunicazioni che, quindi, non avvengono direttamente a livello degli operatori sanitari nazionali, assicurano una maggior tutela dei dati personali degli assistiti e seguono il modello "*business to business*". Nel "*cicle of trust*", i "*National Contacts Point*" si servono di "*Trasport Layer Security*" (TL/SSL)[109] per le comunicazioni tra gli Stati, e, VPN

---

[105] "*The circle of trust*" è inteso come "*the agreed framework for creating trust by establishing policies for critical data protection, privacy and confidentiality issues as well as mechanisms for their audit (FR02 & NFR09 Trust between countries definition)*" in ivi, p. 29.

[106] Ivi, p. 17.

[107] Servizi garantiti da "*the NCP_Security_Service_epSOS*", "*the NCP_Security Service_National*", "*the HCP_Confirmation_Service*" (*cfr.* SMART OPEN SERVICES FOR EUROPEAN PATIENTS, *Open eHealth initiative for a European large scale pilot of Patient Summary and electronic Prescription, D3.3.2 Final epSOS, System Technical Specification, D3.3.2_v1.4*, WP3.3, D3.3.2_v1.4, 28.04.2010, p. 70).

[108] Ad esempio attraverso "*the NCP_Audit_Service*" (*cfr*. ivi, p. 69).

[109] SMART OPEN SERVICES FOR EUROPEAN PATIENTS, *Open eHealth initiative for a European large scale pilot of Patient Summary and electronic Prescription, D3.3.3 epSOS Interoperability Framework, D3.3.3_v. 2.3*, D3.3.3_v.2.3, 15.04.2010, pp. 30 ss.

(ipSEC)[110] per proteggere i flussi di dati e firmare le asserzioni (o autorizzazioni) SAML[111].

Il ruolo che, dunque, è affidato ad un NCP è centrale per realizzare, in modo efficiente ed efficace, l'interoperabilità transnazionale; le funzioni che esso assolve sono plurime. A titolo esemplificativo, nel meccanismo di scambio dei dati - dati che, peraltro, devono essere identificati in modo univoco da parte dei sistemi nazionali -, un NCP può svolgere ora il ruolo di *provider* (se agisce al fine di "*Retrive operation*"), ora quello di *consumer* (se, invece, opera per "*Query operation*"); in entrambi i casi è, però, importante che i requisiti semantici e linguistici dei sistemi, "emittente" e "ricevente", siano rispettati[112]. Ma vi è di più. Affinché tale risultato sia raggiungibile è indispensabile la condivisione di *standard*, possibile anche grazie all'interazione tra gli attuali organismi di normazione e l'industria.

Il progetto *epSOS* parte dall'assunto per cui l'interoperabilità semantica implica che i dati scambiati nel contesto pan-europeo richiedono di essere tradotti nel linguaggio del ricevente, ove con linguaggio è da intendersi la lingua, la semantica, ma anche la stessa struttura dei dati[113]. Considerata l'eterogeneità degli *standard* semantici utilizzati dagli Stati *partner* del Progetto - sebbene molti di essi adottino SNOMED-CT e ICD-10 -, lo *standard* individuato per la descrizione dei "*data element*" di un documento, è HL7 CDA (*Clinical Document Architecture*), con vincoli aggiuntivi a HL7 *Continuity of Care Document* (CCD)[114] e IHE *Patient Care Coordination* (IHE PCC)[115]. I motivi della scelta sono attribuiti alla diffusa adozione da parte dei sistemi informativi sanitari nazionali di questo *standard*, nonché alla sua facilità (e, di conseguenza, rapidità) di implementazione e compatibilità con le soluzioni industriali esistenti. In breve (maggiori dettagli su HL7 CDA

---

[110] *Ibidem*.

[111] "*Security Assertion Markup Language*" (SAML) è uno *standard* per lo scambio di dati di autenticazione e autorizzazione tra domini di sicurezza distinti. SAML è definito e mantenuto da OASIS "*Security Services Technical Committee*", il cui operato è consultabile all'indirizzo https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security.

[112] A tal fine sono stati predisposti i seguenti servizi: "*NCP_Semantic_Service*", "*NCP_Localisation_Services*", "*NCP_Message_Adapter*" (*cfr*. ivi, pp. 71).

[113] SMART OPEN SERVICES FOR EUROPEAN PATIENTS, *Open eHealth initiative for a European large scale pilot of Patient Summary and Electronic Prescription, Work Package 3.5 - Semantic Services Definition*, D3.5.2_v. 0.0.6, 31.05.2010, pp. 103.

[114] Maggiori informazioni su HL7 CDA e CCD sono disponibili nella sezione dedicata agli *standards* del sito *web* di HL7 e precisamente alla pagina http://www.hl7.org/implement/standards/index.cfm?ref=nav.

[115] Per approfondimenti si rinvia a: "*Integrating the Healthcare Enterprise, Patient Care Coordination (PCC) Technical Framework (TF) Revision 5.0*", 2009, Vol. 2; "*IHE Patient Care Coordination Technical Framework Supplement. CDA Content Modules Trial Implementation*", 2009; "*HL7 Implementation Guide: CDA Release 2 – Continuity of Care Document (CCD)*, 2007; "*HL7 Implementation Guide for CDA Release 2: History and Physical (H&P) Notes (U.S. Realm). Draft Standard for Trial Use, Release 1, Levels 1, 2, and 3*", 2008.

sono, infatti, forniti nella presentazione del progetto avviato dall'Austria "*ELGA - Elektronische Gesundheitsakte*"): elementi strutturali di un documento CDA sono l'"intestazione", che identifica e classifica il documento e dà informazioni sull'autenticazione, la visita, il paziente, e gli operatori coinvolti[116], nonché il "corpo" o contenuto clinico, che, può essere "non strutturato" o "strutturato", se suddiviso in sezioni annidate[117].

Con riferimento al problema della lingua - e cioè al fatto che i documenti sanitari sono sì in genere redatti nella lingua madre dell'operatore sanitario, ma, ai fini dell'interoperabilità, essi devono poter essere letti dal ricevente nel proprio codice linguistico -, in *epSOS*, è stato scelto un solo "*code system*" per "*code element*" e ciò, soprattutto perché non esiste alcuna mappatura ufficiale tra i sistemi di codifica esistenti. Ogni elemento codificato ha, pertanto, solo un sistema di codice associato, abbinato al proprio nome visualizzato in lingua inglese. Il catalogo finale ("*epSOS Master Value Set Catalogue*") costituisce la base per l'ontologia *epSOS*[118] e per il catalogo "*epSOS Master Translation/Transcoding*" (*epSOS MTC*). Quest'ultimo, a sua volta, fornisce i mezzi per il "*cross reference*" tra i sistemi di codifica e per la traduzione del nome di visualizzazione.

Altrettanto rilevante è, poi, la questione semantica dei termini utilizzati; in proposito, obiettivo di *epSOS* è quello di sviluppare servizi semantici transfrontalieri interoperabili. Considerata l'assenza di precedenti analoghi, punto di partenza sono stati i termini utilizzati in un contesto piuttosto specifico come la "*European Emergency Card*" per "*Patient Summary*" nonché quelli più comunemente adoperati per "*ePrescription*"[119].

Ritornando alle molteplici attività che si compiono a livello di *National Contact Point*, altrettanto significativa la funzione di un NCP (ad esempio B) per l'autenticazione dell'identità del *provider* (operatore sanitario di B). Tale funzione di "garante dell'autenticità" dello scambio dei dati che un "*National Contact Point*" assume è principalmente possibile grazie al fatto che le firme digitali sono rilasciate proprio a livello

[116] Ivi, p. 15. Scopo dell'intestazione CDA è consentire lo scambio di documenti clinici tra e all'interno delle istituzioni, facilitare la gestione clinica dei documenti e la loro compilazione.

[117] Ogni sezione può contenere un unico blocco narrativo e un numero qualsiasi di voci CDA e riferimenti esterni, che, certamente, devono essere leggibili e processabili.

[118] *Cfr.* SMART OPEN SERVICES FOR EUROPEAN PATIENTS, *Open eHealth initiative for a European large scale pilot of Patient Summary and Electronic Prescription, Work Package 3.5 - Semantic Services Definition Appendix E - Ontology Specifications*, D3.5.2_v. 0.3, February 23rd, 2010, pp. 9.

[119] Per approfondimenti su "*The terminology access services*" si rinvia a SMART OPEN SERVICES FOR EUROPEAN PATIENTS, *Open eHealth initiative for a European large scale pilot of Patient Summary and Electronic Prescription, Work Package 3.5 - Semantic Services Definition*, D3.5.2_v. 0.0.6, 31.05.2010, pp. 28 ss.

di NCP[120]. In aggiunta a ciò, per garantire la sicurezza all'intero del sistema, tutti i dati sanitari sono criptati durante il passaggio tra *gateway* e tutti gli accessi ai dati sono tracciati con i sistemi di "*audit trail*".

Fondamentale è, poi, il ruolo che un NCP assume nel processo di identificazione del paziente, identificazione che è indispensabile avvenga in modo univoco. Proprio a livello di NCP si completa tale processo, che, più frequentemente, inizia nel Paese di provenienza del paziente ma che, talora, può realizzarsi in un Paese terzo.

Il collegamento, sincronizzato, tra il nodo NCP ed i domini nazionali nonché quello tra il nodo NCP ed il dominio *epSOS* avviene attraverso le interfacce NCP nazionali, strumenti imprescindibili per rendere possibili le funzioni di interoperabilità[121].

Affinché l'interoperabilità prevista sia raggiunta in modo adeguato, è, altresì, essenziale che, sia a livello nazionale sia a livello transnazionale, siano messe in atto le prescrizioni sulla sicurezza esistenti da parte di tutte le organizzazioni coinvolte; ciò implica non soltanto l'utilizzo di strumenti per rendere i dati sicuri (come, ad esempio, firme digitali, certificazioni, sistemi per la crittografia), ma anche l'adozione di diverse funzioni manageriali ("*service managment*" e "*service logging*") e relativi *standard* ("*Web Services Security Standard*" - "*WS-Security*", "*WS-Trust*" -)[122].

Altro importante compito affidato a "*National Contact Point*" è relativo alla validazione del rilascio di consenso al trattamento dei dati sanitari: in particolare, nel nodo NCP si conclude la decisione finale se accogliere o meno il consenso rilasciato dal paziente in uno Stato diverso da quello di propria provenienza. Nel rispetto del principio di

---

[120] In proposito sono, tuttavia, necessarie alcune precisazioni: nel caso di "*Query response*" e "*Notification Response*" non è necessaria alcuna firma; nel caso, invece, di "*Retrive response*", NCP-A imbusta i dati medici e firma dell'HCP, aggiungendo la propria firma, NCP-B può in via opzionale firmare la risposta di documento ricevuto da rinviare a HCP; nel caso di "*eDispense*", NCP-B imbusta dati sanitari e firma del HCP e aggiunge la sua stessa firma, NCP-A può in via opzionale firmare la risposta di documento ricevuto da rinviare a HCP. I metadati sono protetti dal messaggio di sicurezza.

[121] In particolare, l'interfaccia che collega il nodo NCP al dominio nazionale (NCP_IF_National) è composta dalle seguenti "sub-interfacce": (i) "IF_PID_Requestor", prevista per richiedere l'ID del paziente, (ii) "IF_Medical_Data", usata per le applicazioni *ePrescription* e *Patient Summary*, (iii) "IF_HCP_ID_Provider", adoperata per richiedere una "HCP identity assertion". L'interfaccia che, invece, collega il nodo NCP al dominio epSOS è composta da due "sub-interfacce": (i) "IF_Medical_Data", usata per richiedere i dati clinico-sanitari e (ii) "IF_PID_Registry", utilizzata per "PID information". In SMART OPEN SERVICES FOR EUROPEAN PATIENTS, *Open eHealth initiative for a European large scale pilot of Patient Summary and electronic Prescription, D3.3.2 Final epSOS, System Technical Specification, D3.3.2_v1.4*, WP3.3, D3.3.2_v1.4, 28.04.2010, pp. 73 ss.

[122] SMART OPEN SERVICES FOR EUROPEAN PATIENTS, *Open eHealth initiative for a European large scale pilot of Patient Summary and electronic Prescription, D3.3.3 epSOS Interoperability Framework, D3.3.3_v. 2.3*, D3.3.3_v.2.3, 15.04.2010, pp. 25 ss. Per quanto concerne considerazioni giuridiche elaborate all'interno del progetto epSOS si rinvia a: SMART OPEN SERVICES FOR EUROPEAN PATIENTS, *Open eHealth initiative for a European large scale pilot of patient summary and electronic prescription, Key Task 2.1.1 - Legal and Regulatory Requirements at EU level*, document version: final, 2012, pp. 47.

minimizzazione nel trattamento di dati "sensibili", il processo di verifica del consenso che inizia in NCP A precede il processo semantico. In *epSOS,* per tutti i documenti scambiati, è sufficiente un solo consenso[123]; sono, inoltre, ammessi solo due tipi di autorizzazioni:

(i) "*a sign XML assertion*", tale consenso viene creato tra "NCP" e "Paese A" ed aggiunto alla transazione al momento dello scambio;

(ii) "*a PDF document*": rappresenta il consenso originale rilasciato dal paziente nel proprio "Paese di origine" e dev'essere obbligatoriamente reso noto al "Paese B" in caso di richiesta.

4.2 AUSTRIA

Ottemperando a quanto indicato nel 2004 dalla Commissione Europea ne "*eHealth Action Plan*", l'anno seguente il Governo austriaco varò una nuova legge sanitaria nazionale per la riforma del sistema, con la quale, tra l'altro, fu prevista l'introduzione di *Information and Communication Technology* in sanità[124].

Primi risultati di tale adozione furono "*eCard*" predisposte per l'individuazione di un'identità elettronica dei cittadini austriaci finalizzata all'assicurazione sanitaria ed alla sicurezza sociale. L'infrastruttura sottesa a questi seppur importanti strumenti digitali non era, tuttavia, sufficientemente compatibile con la memorizzazione di ogni tipologia di informazioni e dati sanitari.

Per tale ragione, apparve, allora, fondamentale implementare un sistema informativo sanitario nazionale in grado di mettere in atto le nuove richieste della Commissione europea; in questo contesto si colloca il progetto "*ELGA - Elektronische Gesundheitsakte*" (*ELGA*)[125].

[123] L'accesso senza il consenso del paziente in casi salvavita nei quali non è possibile che sia prestato consenso, segue le stesse regole dell'accesso al pronto soccorso: HCP B manda la richiesta di autenticazione a NCP-A.

[124] *Gesundheitsreformgesetz 2005*, Bundesgesetzblatt für die Republik Ősterreich, Jahrgang 2004, Ausgegeben am 30, Dezember 2004, Teil I, 179. Bundesgesetz.

[125] La *homepage* del Progetto è disponibile all'indirizzo http://www.elga.gv.at/. Ulteriori informazioni su "ELGA" sono accessibili nel sito del Ministero federale della sanità austriaco ("*Das Bundesministerium für Gesundheit*") e sul Portale della salute ("*Das öffentliche Gesundheitsportal Österreichs*"), rispettivamente consultabili agli indirizzi http://www.bmg.gv.at/ e https://www.gesundheit.gv.at.

4.2.1 PROGETTO "*ELGA*"[126]

Avviato nel 2006[127], dopo un lungo *iter* di preparazione, il progetto "*ELGA - Elektronische Gesundheitsakte*" è stato, con maggior continuità, sviluppato a partire dal novembre 2009 con la fondazione di "*ELGA GmbH*", organizzazione *no-profit* di interesse pubblico, costituita per la predisposizione di servizi in materia di sanità elettronica, e, in particolare, per l'introduzione e l'implementazione di un Fascicolo Sanitario Elettronico nazionale. La piena operatività della prima fase progettuale è prevista per il 2017; infra quella data, sono, però, fissati diversi *step* intermedi per permettere la graduale diffusione di questo strumento di *e-Health* in ospedali pubblici e case di cura, ma anche presso uffici sanitari, farmacie, dentisti, medici di medicina generale e pediatri.

Dal 1° gennaio 2013 è in vigore la nuova legge austriaca in materia di telematica sanitaria che, ufficialmente, prevede l'introduzione del nuovo sistema informativo sanitario, "*Elektronische Gesundheitsakte - ELGA*", volto, appunto, a garantire un flusso incrociato di informazioni e dati tra gli operatori sanitari (ospedali, medici, farmacie) e pazienti[128]. In particolare, secondo quanto statuito nella legge invocata, *ELGA* consentirà l'accesso alle informazioni sanitarie, indipendentemente dalla loro localizzazione o dal momento della loro generazione, migliorando la qualità e l'efficienza dell'assistenza sanitaria erogata. La partecipazione, totale o parziale, del paziente austriaco a questo sistema informativo è facoltativa[129].

Per il raggiungimento di tali risultati, obiettivo primario è la realizzazione di una piattaforma sicura per lo scambio, in formato elettronico, di informazioni riguardanti i pazienti, sia quelle contenute nelle prescrizioni mediche elettroniche sia, più in generale,

---

[126] Una conoscenza dettagliata de "*die elektronische Gesundheitsakte*" (*ELGA*) è stata possibile grazie al tirocinio formativo (29 gennaio - 30 aprile 2013), svolto da Maria Gabriella Virone presso la *University of Applied Sciences Technikum Wien - Biomedical Engineering Sciences Department* e sovvenzionato da una borsa di studio "*Lifelong Learning Programme* 2007/2013 - *Erasmus Placement* a.a. 2012-2013" erogata da Alma Mater Studiorum Università di Bologna. Particolare gratitudine ai professori A. Mense ("*Head of Department of Information Engineering & Security*" - "*Program Director Information Management und IT Security*") e S. Sauermann ("*Program Director Biomedical Engineering Sciences*") per l'ospitalità e per aver permesso la collaborazione con il *Team* del progetto "*Health Interoperability*" (la cui *homepage* è disponibile all'indirizzo http://www.healthy-interoperability.at/).

[127] Proprio nel 2006 è stato definito lo studio di fattibilità del Progetto; *cfr*. IBM ÖSTERREICH GMBH, *Machbarkeitsstudie betreffend Einführung der elektronischen Gesundheitskarte (ELGA) im österreichischen Gesundheitswesen*, Endbericht, 21 November 2006.

[128] *Elektronische Gesundheitsakte-Gesetz - ELGA-G*, Bundesgesetzblatt für die Republik Österreich, Jahrgang 2012, Ausgegeben am 14, Dezember 2012, Teil I, 111. Bundesgesetz.

[129] Per approfondimenti sulla legislazione austriaca sul trattamento dei dati sanitari personali contenuti nel Fascicolo Sanitario Elettronico si rinvia a S. REIMER, *Current and Future Settings of Austrian Legislation Regarding Electronic Health Records (EHR)*, European Journal for Biomedical Informatics - Vol. 8, Issue 2, 2012, pp. 11-28.

tutti i dati concernenti la storia clinico-sanitaria dell'assistito (come risultati di laboratorio, referti radiologici, lettere di dimissioni ospedaliere).

Nella predisposizione di un'architettura volta all'interoperabilità tra il sistema informativo sanitario austriaco e quelli europei è, senza dubbio, importante la partecipazione dell'Austria al progetto "*Smart Open Services for European Patients*"; l'approccio del Progetto pilota ha, infatti, orientato verso la realizzazione di un sistema nazionale che avesse caratteristiche tecniche analoghe.

Non secondario, inoltre, il ruolo che l'iniziativa "*Integrating the Healthcare Enterprise*" ha avuto per la realizzazione di *ELGA*; nel 2007, infatti, la Commissione federale della sanità ha raccomandato l'adozione di IHE come *framework* di riferimento per il disegno dell'infrastruttura di base. In particolare, per il processo dei dati, *ELGA* adotta per lo più le componenti (o "*Integrating Profile*") suggerite da IHE; rilevanti sono le seguenti: CT ("*Consistent Time*"), ATNA ("*Audit Trail and Note Authentication*"), PDQ ("*Patient Demography Query*"), PIX ("*Patient Identifier Cross Referencing*"), BPPC ("*Basic Patient Privacy Consent*"), XUA ("*Cross Enterprise User Assertion*"), XCA ("*Cross Community Assertion*"), XDS a+b ("*Cross Enterprise Document Sharing*").

Per quanto attiene alla struttura dei documenti clinici, in ELGA sono utilizzati *HL7* "*Reference Information Model*" (RIM) e HL7 CDA ("*Clinical Documentation Architecture*")[130].

Gli identificativi di laboratorio e le immagini mediche seguono rispettivamente gli *standard* "*Logical Observation Identifiers Names and Codes*" e "*Digital Imaging and Communications in Medicine*".

Le politiche di sicurezza per il controllo degli accessi adottano, invece, lo *standard* "*eXtensible Access Control Markup Language*" (XACML), definito dal Consorzio OASIS

[130] In ELGA, *standard* di riferimento sono: (i) per l'architettura delle comunicazioni: INTEGRATING THE HEALTHCARE ENTERPRISE - TECHNICAL FRAMEWORK (*IT Infrastructure Technical Framework*, rev. 3.0, 2006; *Patient Care Coordination Technical Framework*, rev. 1.0; *Laboratory Technical Framework*, rev. 1.1, 2004; *Radiology Technical Framework*, rev. 7.0, 2006); (ii) come *basic data model*: HL7, VERSION 3, RIM (*ISO/HL7 21731:2006(E), Health informatics - HL7 version 3 - Reference Information Model - Release 1*); (iii) come *standard* per i documenti: HL7, *Clinical Document Architecture (CDA), Rel. 2* (*ANSI/HL7 CDA, R2-2005*); (iv) per i dati di laboratorio: *Logical Observation Identifiers Names and Codes* (*LOINC® 2.19:2006-12-22*); (v) per le immagini radiologiche: DICOM 3.0 e WADO (*ISO 12052:2006(E), Health informatics - Digital imaging and communication in medicine (DICOM) including workflow and data management*; *ISO 17432:2004(E), Health informatics - Messages and communication - Web access to DICOM persistent objects*).

("*Organization for the Advancement of Structured Information Standards*")[131] e basato su XML[132].

4.2.1.1 "*INTEGRATING THE HEALTHCARE ENTERPRISE INTEGRATION PROFILES*"

Prima di entrare nel merito dell'architettura di *ELGA* (*cfr. figg.* 6 e 7), è essenziale, anzitutto, soffermarsi brevemente sulle principali caratteristiche delle componenti di "IHE" summenzionate[133].

"*Consistent Time Integration Profile*" (CT) è un meccanismo di sincronizzazione tra gli attori (*server* e *client*) coinvolti in un sistema informativo sanitario.

"*Audit Trail and Node Authentication Integration Profile*" (ATNA), analogamente a quanto in generale definito da procedure e *policy* sulla sicurezza, individua le misure di sicurezza finalizzate a garantire la riservatezza e l'integrità dei dati dei pazienti nonché la responsabilità degli utenti. Esso contiene informazioni relative agli elementi di sicurezza adottati a livello di "*Basic Secure Node*", definisce i requisiti minimi di verifica per singolo nodo (come identificazione dell'utente e della macchina, autenticazione, autorizzazione, controllo degli accessi etc.) nonché i requisiti minimi di sicurezza per le comunicazioni del nodo; stabilisce, inoltre, le caratteristiche della comunicazione dei messaggi di verifica tra "*Basic Secure Node*" e "*Audit Repository Node*", nei quali sono raccolte le informazioni di verifica.

"*Patient Demographics Query Integration Profile*" (PDQ) consente di reperire, grazie alla predisposizione di specifici criteri di ricerca, in una lista di soggetti, informazioni "demografiche" relative ad un singolo paziente.

"*Patient Identifier Cross-referencing Integration Profile*" (PIX) fornisce un nuovo identificativo del paziente frutto dell'incrocio di identificativi dello stesso soggetto provenienti da più "*Patient Identifier Domain*"; grazie al PIX è possibile raccogliere informazioni sanitarie provenienti da fonti diverse relative al medesimo assistito.

"*Basic Patient Privacy Consents Integration Profile*" (BPPC) identifica un meccanismo per registrare il consenso del paziente al trattamento dei dati personali ed individua un

---

[131] Dettagliate informazioni sul Consorzio e sull'attività da esso svolta sono disponibili nella *homepage*, consultabile all'indirizzo https://www.oasis-open.org/; per ulteriori approfondimenti su XACML si rinvia, invece, alla sezione del sito *web* dedicata alla *Technical Committee*, consultabile all'indirizzo https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml.

[132] Maggiori informazioni su "*eXtensible Markup Language*" (XML) sono reperibili all'indirizzo http://www.w3.org/XML/.

[133] Per quanto concerne la descrizione dei singoli *workflow* si rinvia integralmente al documento INTEGRATING THE HEALTHCARE ENTERPRISE, *IHE IT Infrastructure (ITI) - Technical Framework*, Vol. 1 (ITI TF-1), Integration Profiles, Revision 9.0 – Final Text, August 31, 2012, pp. 255.

metodo per selezionare quale consenso possa essere effettivamente applicato nelle diverse circostanza d'uso.

"*Cross-Enterprise User Assertion Profile Integration Profile*" (XUA) individua un metodo per comunicare a terzi l'identità di un soggetto autenticato all'interno di una azienda sanitaria (*user, application, system* ...). L'accesso dei terzi ai dati in oggetto è, tuttavia, subordinato alla loro identificazione per motivi di responsabilità e garanzia.

"*Cross-Community Access Integration Profile*" (XCA) permette di chiedere e reperire informazioni relative ad un paziente che siano in possesso di realtà sanitarie terze rispetto al richiedente.

"*Cross-Enterprise Document Sharing Integration Profile*" (XDS), basato sugli *standard* "*ebXML Registry*"[134] e "*Simple Object Access Protocol*" (*SOAP*), consente alle organizzazioni aderenti ad un "*XDS Affinity Domain*" di scambiare cartelle clinico-sanitarie in forma di documenti[135]. Anche in questo caso, beneficiari finali di tale organizzazione sono i pazienti, i quali, in un'ottimale scenario, possono godere di processi di cura più adeguati, proprio grazie alla cooperazione di più specialisti.

4.2.1.2 "*HL7 REFERENCE INFORMATION MODEL*" E "*HL7 CLINICAL DOCUMENTATION ARCHITECTURE*"

Come in precedenza indicato, in *ELGA* la struttura dei documenti clinici utilizza il modello concettuale di riferimento "*HL7 Reference Information Model*" (RIM) e lo *standard* "*HL7 Clinical Documentation Architecture*" (CDA)[136].

"*HL7 Reference Information Model*" è il modello di rappresentazione di dati clinici sviluppato da "*Health Level 7*"; fondato su "*Unified Modeling Language*", RIM fornisce una rappresentazione esplicita delle connessioni semantiche e lessicali che possono esistere nei messaggi HL7. La prima bozza di "*Reference Information Model*" fu rilasciata nel 1996, la versione 1.0 è, invece, del 2001; nel 2003 HL7 RIM è diventato uno *standard* ANSI ("*American National Standards Institute*") e nel settembre 2006 è stato pubblicato

---

[134] *Electronic Business using eXtensible Markup Language* è una famiglia di *standards* prodotta da OASIS e UN/CEFAT per lo scambio di informazione nei domini di commercio elettronico. Maggiori informazioni sono disponibili nel sito *web* dedicato, consultabile all'indirizzo http://www.ebxml.org/.

[135] Il concetto di "*Affinity Domain*" si riferisce ad un gruppo di aziende sanitarie che, accettando di lavorare congiuntamente, condividono *policy* - ad esempio relative alle modalità di identificazione del paziente, di rilascio ed uso del consenso - e regole - concernenti il formato, il contenuto, la struttura, l'organizzazione e la rappresentazione di informazioni cliniche etc. -.

[136] Ulteriori approfondimenti su HL7 RIM e HL7 CDA sono disponibili nelle sezioni dedicate del sito di *Health Level Seven*, rispettivamente consultabili agli indirizzi: http://www.hl7.org/implement/standards/rim.cfm e http://www.hl7.org/implement/standards/product_brief.cfm?product_id=7.

come *standard* da parte di "*International Organization for Standardization*". Attualmente "*HL7 Reference Information Model*" è utilizzato con sistemi di codifica, quali "*Systematized Nomenclature of Medicine - Clinical Terms*" (SNOMED CT) e "*Logical Observation Identifiers Names and Codes*" (LOINC®) per definire concetti medici nello *standard* "*HL7 Clinical Documentation Architecture*".

"*HL7 Clinical Documentation Architecture*" è uno *standard* internazionale certificato, utilizzato per specificare codice, struttura e semantica dei documenti clinico-sanitari. Ideato dal Comitato Tecnico "*Structured Documents*" (la *Release* 1.0 fu pubblicata nel 2000, la versione 2.0 nel 2005), CDA ha lo scopo di favorire l'interoperabilità tra i documenti nel dominio in esame[137]. Basato sul linguaggio di marcatura XML, tale *standard* può essere facilmente supportato da qualsiasi applicazione.

Parti essenziali della struttura di un documento CDA sono "*header*" e "*body*": il primo fornisce le meta-informazioni che identificano e classificano il documento, quali informazioni relative ad autenticazione ("*document information*"), visita ("*encounter*"), paziente ("*service target*") e operatori coinvolti ("*service actor*")[138]; il secondo contiene il rapporto clinico e può essere "non strutturato" o "strutturato", se, oltre al "blocco narrativo", contiene ulteriori sezioni annidate che sono utilizzate per specificarlo (è il caso di "*entry*", quali, ad esempio "*observation*") o per codificare porzioni esterne richiamate nel testo, come immagini (è il caso di "*external reference*")[139].

Interessante, altresì, evidenziare il concetto di interoperabilità semantica c.d. "incrementale" presente in "*HL7 Clinical Document Architecture*", secondo cui un documento clinico può essere appunto ampliato nel tempo, aggiungendo al modello base, strutturalmente più semplice, ulteriori elementi. Il risultato finale di tale progressiva incrementazione della struttura è una maggiore automazione dei processi e, di conseguenza, una più ampia interoperabilità tra i sistemi informativi.

---

[137] In HL7 un documento clinico deve avere le seguenti sei caratteristiche: persistenza, amministrazione, potenziale per l'autenticazione, contesto, totalità, leggibilità umana.

[138] L'*header* del documento contiene, ad esmepio, le seguenti informazioni: *id*: Identificativo univoco del documento; *code*: Codifica LOINC; *effectiveTime*: Data di creazione del documento; *author*: Persona che valida il documento; *custodian*: Struttura che ha generato il referto; *recordTarget*: Anagrafica Paziente; *title*: Testo d'intestazione del documento; *setId*: Identificativo comune ad ogni revisione del documento; *versionNumber* : Versione del documento; *legalAuthenticator*: Firmatario del referto; *informationRecipient*: Unità di consegna; *dataEnterer*: Rappresenta la persona che inserisce i dati nel sistema; *responsibleParty*: Primario della struttura che ha generato l'atto; *relatedDocument*: Collegamento tra due documenti; *documentationOf*: Motivo della richiesta di indagine; *inFulfillmentOf*: Order Filler; *componentOf*: Order Placer e Unità richiedente.

[139] In "Appendice" si riporta un esempio, alquanto semplificato, di documento redatto tenendo presente le indicazioni di HL7 CDA; segue, poi, la visualizzazione dello stesso documento secondo il foglio di stile adottato nel progetto ELGA.

A titolo esemplificativo, i livelli di interoperabilità semantica incrementale possibili sono tre: in tutti e tre i casi sono rispettati i requisiti previsti dal "*CDA XML Schema*". Se, per quanto concerne l'*header*, i documenti sono sostanzialmente analoghi, alcune differenze sostanziali tra i tre livelli si osservano nel *body*. Infatti, mentre a livello "uno" il testo del rapporto clinico è "umanamente leggibile", a livello "due" il "*body*" è espressivamente più ricco è più facilmente "*machine-readable*", principalmente grazie al fatto che sezioni/sottosezioni codificate in forma più specifica e dettagliata; il livello "tre", infine, in aggiunta contiene ulteriori specifiche che rendono, pertanto, il documento qualitativamente migliore per essere trattato in forma automatizzata (secondo quanto indicato in HL7 RIM)[140].

4.2.1.3 "*eXTENSIBLE ACCESS CONTROL MARKUP LANGUAGE*"

Considerata la natura fortemente sensibile dei dati oggetto dei sistemi informativi sanitari, particolarmente importante è l'implementazione di sistemi di autorizzazione e controllo degli accessi ai documenti; per la definizione di tali politiche di sicurezza, *ELGA* utilizza lo *standard* "*eXtensible Access Control Markup Language*" (XACML).

In XACML, ciascuna politica di accesso ai dati sanitari (*policy*) è costituita da un *target* (ovvero il soggetto destinatario della regola) e da un insieme di regole o *rule* (ciascuna costituita da un *target*, un effetto o decisione - permesso o diniego -, ed una condizione - il cui scopo è restringere l'applicabilità di una regola -[141]). Affinché i risultati di una regola possano correttamente essere applicati per ottenere una decisione finale della *policy*, sono predisposti algoritmi di combinazione.

Quanto premesso è strumentale per comprendere il meccanismo di funzionamento delle componenti dell'architettura proposta da XACML: "*Policy Enforcement Point*" intercetta le richieste di accesso alle risorse (eventualmente includendovi gli attributi del soggetto, della risorsa e dell'ambiente reperiti da "*Policy Information Point*"), per poi inoltrarle a "*Policy Decision Point*", cui spetta, invece, la valutazione delle *policies* applicabili (*policies* conservate in un *repository* e prodotte da "*Policy Administration Point*") e la successiva decisione. In caso di autorizzazione, "*Policy Enforcement Point*" esegue la richiesta di accesso.

---

[140] Per approfondimenti, tra gli altri, vedasi: R.H. DOLIN, L. ALSCHULER, S. BOYER, C. BEEBE, F. M. BEHLEN, P. V. BIRON, A. SHABO, *HL7 Clinical Document Architecture, Release 2*, Journal of the American Medical Informatics Association, 2006; 13(1): 30-39.

[141] L'effetto o decisione è un requisito obbligatorio all'interno di una regola, contrariamente alla condizione che è facoltativa.

4.2.1.4 ARCHITETTURA PROGETTO "*ELGA*"

Inquadrati gli *standard* dei quali *ELGA* si serve, di seguito sono descritte l'architettura e l'infrastruttura utilizzate dal sistema informativo sanitario austriaco, nel quale, la componente centrale funge da ponte di collegamento con i sistemi informativi locali (del singolo ospedale, di un *cluster* di ospedali o "*Lokale Affinity Domains*", del singolo medico curante) (come sinteticamente illustrato nelle *figure* 6 e 7).

Componenti centrali di *ELGA* sono "*Zentraler Patientenindex*" o "*Master Patient Index*" (ZPI), "*Gesundheitsdiensteanbieter-Index*" o "*Healthcare Provider Index*" (HPI), "*Portal*" o "*Consumer Portal*" (C Portal), "*Protokollierungssystem*" o "*Protocol Datawarehouse*", "*Policy Administration Point*" (PAP), "*ELGA Token Service*" (ETS)[142] (*cfr. fig. 6*).

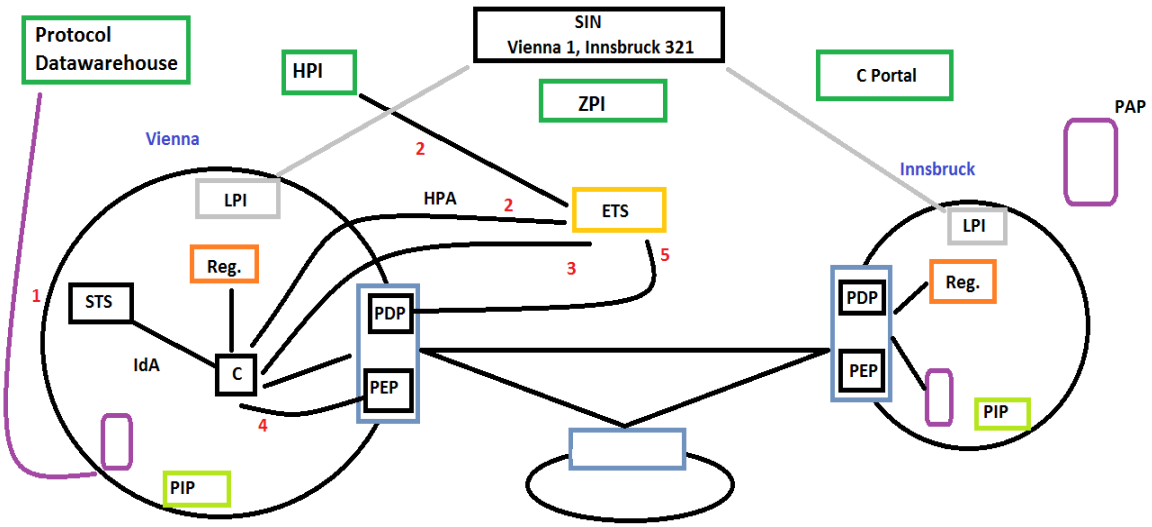


Figura 6 - ELGA Information Security System

"*Master Patient Index*" è lo strumento che consente l'identificazione univoca del paziente: utilizzando *PIX Integration Profile*, gli identificativi assegnati a livello di "*Local Patient Index*" nei "*Local Affinity Domain*" (e.g. Vienna e Innsbruck), sono riconosciuti come relativi alla medesima persona e, quindi, riunificati.

"*Healthcare Provider Index*" (HPI) è una raccolta di dati identificativi di "*Healthcare Provider*" e/o loro dipendenti; grazie a questo strumento, come si dirà, è possibile verificare se e quali soggetti sono autorizzati ad accedere (e a quali) dati, tutelando così la riservatezza dei pazienti.

[142] Gli acronimi riportati tra parentesi corrispondono a quelli utilizzati in *figura 6*.

Altra componente centrale di *ELGA*, che può, peraltro, essere presente anche a livello di singoli "*Local Affinity Domain*", è "*Policy Administration Point*" (PAP), preposta alla gestione del "diritto di accesso", parziale o totale, dei pazienti; in PAP, infatti, sono conservati i documenti contenenti il rilascio del consenso dei pazienti (in questo caso è utilizzato il "*Basic Patient Privacy Consents Integration Profile*").

"*Protocol DataWareHouse*" funge da sistema di protocollo generale per l'*auditing*: sincronizzato con i "*Local Data Audit Repository*", è interrogato per verificare una "*Identity Assertion*", ossia l'identità di un soggetto, evitando, così, possibili frodi.

"*Consumer Portal*" è predisposto a beneficio degli utenti finali, ovvero i cittadini/pazienti, i quali, attraverso il Portale possono accedere ai propri dati personali contenuti nel Fascicolo Sanitario Elettronico, gestire i documenti di rilascio del consenso, acquisire informazioni sui "PAP" e così via.

"*ELGA Token Service*" è il meccanismo di autenticazione tra servizi; a tal fine, esso utilizza "*Security Assertion Markup Language*" (*SAML*). Di seguito si illustrano le modalità in cui è stato progettato il procedimento di autorizzazione in *ELGA*.

Quando un soggetto "C" ("*document consumer*") desidera consultare un documento clinico contenuto in un altro sistema informativo sanitario (e.g. Innsbruck), affinché possa venirne in possesso, occorre che ne faccia richiesta al "*Registry*" del proprio "*Local Affinity Domain*" (e.g. Vienna), che, grazie ai metadati in proprio possesso, verifica l'esistenza (ed, in caso positivo, la localizzazione) del documento stesso. A questo punto, esaurite le fasi di verifica di seguito illustrate, ne fa richiesta, tramite "*Gateway*", al sistema informativo terzo (Innsbruck) che, accertata la compatibilità tra le proprie *policies* e quelle del richiedente, ne invia copia al "*repository*" istante (Vienna).

Prima di effettuare la propria richiesta al "*Registry*" è, tuttavia, indispensabile che il "*document consumer*" venga autenticato da "*Security Token Service*" (STS), ricevendo, quindi, l'autorizzazione all'accesso (nella forma di "*security token*" di tipo SAML). Questa prima fase del procedimento di autorizzazione prende il nome di "*Identity Assertion*". Il "*Security Token Service*" (STS), vera e propria "*Authority*" presente nel "*Local Affinity Domain*", gestisce, dunque, il riconoscimento dell'utente, e, di conseguenza, le politiche di sicurezza del sistema.

Momento successivo è rappresentato da "*Healthcare Provide Assertion*": "C" invia la propria richiesta a "*ELGA Token Service*" che, a sua volta, ricorre a "*Healthcare Provider Index*" per accertare l'identità del richiedente, identificato come soggetto appartenente a quella determinata struttura ospedaliera. Compiuto positivamente questo accertamento, la

fase successiva, nota come "*Patient Assertion*", è quella in cui "*ELGA Token Service*" riconosce che "C", medico appartenente alla struttura ospedaliera "*x*" è il soggetto autorizzato dal paziente "Caio".

Analogamente a quanto già indicato per il progetto *epSOS*, e cioè che le comunicazioni fra sistemi informativi sanitari avvengono esclusivamente attraverso i *National Contact Point*, anche tra "*Local Affinity Domain*" le comunicazioni/scambio di documenti sono possibili esclusivamente attraverso "*Gateway*".

Funzione principale del "*Gateway*" è quella di verificare che la richiesta di accesso alle informazioni contenute nel proprio sistema informativo rispetti le *policy* in essere nel "*Local Affinity Domain*"; lo *standard* utilizzato per valutare le suddette richieste è "*eXtensible Markup Language Access Control*". In accordo con quanto previsto da XACML, i due "nodi operativi" all'interno del singolo "*gateway*" sono "*Policy Decision Point*" (PDP), nel quale sono memorizzate le *policies* locali e "*Policy Enforcement Point*" (PEP), che ha, invece, la funzione di decidere della conformità o meno di un'istanza alle *policies* in essere, previa consultazione e parere del PDP (ove necessario, il "PDP" può servirsi delle informazioni fornite dal "*Policy Information Point*" presente nel "*Local Affinity Domain*").

Conclusa, dunque, la fase "*Patient Assertion*", inizia lo *step* successivo, cioè, "*Accessing Initiating Gateway*": il "*consumer document*" entra in contatto con il "*Gateway*" del proprio "*Local Affinity Domain*" per essere autorizzato da "PEP"; come anticipato, affinché questo avvenga, è preliminare che "PEP" riceva l'autorizzazione da "PDP". A tal fine "*Policy Decision Point*" interroga "*ETSI Token Service*" - questa fase del procedimento di autorizzazione prende il nome di "*Treatment Assertion*" - per accertare che "C" è il medico del paziente "*x*". Il *framework* di riferimento per le azioni descritte è "*Cross-Community Access Integration Profile*" (XCA) di "*Integrating the Healtcare Enterprise*".

Componenti di base dei sistemi informativi sanitari appartenenti alle singole strutture ospedaliere che fanno parte di un "*Local Affinity Domain*" sono: "*Lokaler Patientenindex*" o "*Local Patient Index*" (LPI), "*Dokumenten-Register*" o "*Document Registry*" (XDS Reg.), "*Lokales Protokollierungssystem*" o "*Local Protocol System*", "*ELGA XCA Gateway inklusive Berechtigungssystem*" o "*ELGA XCA Gateway including authorization system*", "*Audit Record Repositories*"[143] (*cfr. figura 7*).

[143] Gli acronimi riportati tra parentesi corrispondono a quelli utilizzati in *figura 7*.

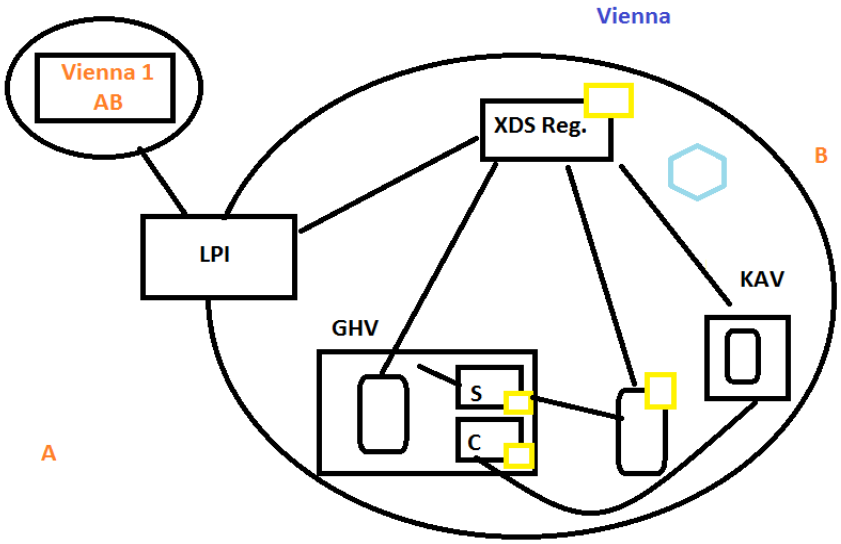


Figura 7 - Local Affinity Domain

"*Local Patient Index*" (LPI) è la raccolta degli identificativi appartenenti ai pazienti curati a livello locale (e.g. Vienna 1 = A+B), generati dagli ID già esistenti (e.g. A e B) nelle strutture ospedaliere (e.g. GHV, KAV) del "*Local Affinity Domain*" (e.g. Vienna). Preliminarmente tali identificativi (con un "*Patient Registration HL7 message*") sono comunicati da LPI al "*Domain Registry*" per consentire di accertare la presenza del paziente nel sistema nonché di verificarne l'identità e, di conseguenza, autorizzare la richiesta dei documenti via "*Gateway*".

I "*CDA document*" perfezionati a livello dei singoli sistemi informativi ospedalieri - nei quali sono presenti "*source*" (S) e "*consumer*" (C) -, sono memorizzati in "*repository*", interni o esterni ai sistemi stessi; i tre attori summenzionati ("*source*", "*consumer*" e "*repository*"), previsti da "*Cross-Enterprise Document Sharing Integration Profile*" (XDS) di "IHE", sono tra loro interoperabili[144].

Al fine di salvaguardare la sicurezza e l'integrità dei dati, ciascuno di questi "soggetti" comunica con gli altri, e con "*Domain Registry*", attraverso "*Secure Nodes Software Authentication*" (secondo quanto previsto da "IHE", in particolare, con il "*Audit Trail and Node Authentication Integration Profile*" (ATNA)[145]. La presenza di un "*Audit Record Repository*" all'interno del "*Local Affinity Domain*" facilita l'implementazione di questi

[144] INTEGRATING THE HEALTHCARE ENTERPRISE, *IHE IT Infrastructure (ITI) - Technical Framework*, cit., pp. 78 ss.
[145] Ivi, pp. 64 ss.

requisiti di sicurezza, il controllo delle transazioni e riduce la possibilità di manomissione dei *record*, e ciò, grazie al fatto che ad esso sono trasferiti tutti gli "*Audit Record*".

Altra componente XDS utilizzata in *ELGA*, è "*Document Registry*" contenente la raccolta di metadati dei "*CDA clinical document*". Questa diversa localizzazione permette di trovare, selezionare e recuperare più facilmente il documento di interesse per la cura del paziente, indipendentemente, quindi, dal risalire al *repository* nel quale, effettivamente, le informazioni sanitarie sono memorizzate[146].

Per quanto, invece, riguarda "*Local Protocol System*" e "*ELGA XCA Gateway including authorization system*", valgono tutte le considerazioni già esposte nella parte precedente dedicata alla descrizione delle componenti centrali di ELGA e dei processi di autentificazione in essere.

Alcune importanti misure nel sistema informativo utilizzato in *ELGA* sono poste, poi, a beneficio dei pazienti austriaci, i quali, ad esempio, possono negare l'accesso ed il trattamento, totale o parziale, dei propri dati sanitari (c.d. *opt-out*) raccolti nel sistema *ELGA*. Altrettanto significativa è, in tal senso, la predisposizione di registri specifici che consentono al paziente di verificare, anche al fine di controllarne gli abusi, gli accessi alle proprie informazioni medico-sanitarie (ad esempio, quali soggetti le hanno consultate, afferenti a quali strutture, in quali tempi etc.). Criterio generale adottato in *ELGA*, come del resto in altri sistemi di *e-Health*, è, infatti, il "*role-based authorization concept*", secondo cui possono avere accesso e trattare i dati del paziente soltanto gli operatori espressamente autorizzati a tali operazioni. Si segnala, fin d'ora, che le modalità di protezione dei dati personali in *ELGA*, rimangono, a tutt'oggi, una delle preoccupazioni più rilevanti per operatori sanitari, pazienti, ma anche tecnici (ingegneri, informatici), *stakeholder* e *policy maker*.

Come menzionato nel paragrafo 4.2.1, dedicato alla presentazione di "*ELGA - Elektronische Gesundheitsakte*", il Progetto è ancora in fase di realizzazione; nonostante l'intensa attività compiuta da "*ELGA GmbH*" per l'attuazione delle regole di autorizzazione e del sistema di registrazione, non è ancora possibile riferire alcun dato sull'utilizzo e diffusione del sistema da parte dei vari soggetti coinvolti nei processi sanitari, siano essi operatori o aziende pubbliche e private. Infatti, se, da una parte, è stato raggiunto un importante risultato, quale la definizione del quadro normativo, con l'entrata in vigore della legge "*Elektronische Gesundheitsakte-Gesetz - ELGA-G*", dall'altra, i

[146] Ivi, pp. 78 ss.

profili organizzativi e di implementazione delle componenti tecniche sono *in fieri*. Per ciò che riguarda proprio la rapidità con cui le componenti tecniche verranno consolidate dai singoli operatori, non è, secondario, altresì ricordare che, mentre alcuni blocchi dell'archiettura di *ELGA* sono sviluppati a livello centrale, altri sono sviluppati a livello locale o regionale, aspetto questo che inevitabilmente condiziona l'omogena ed eguale diffusione del sistema. Occorrerà, dunque, attendere la piena entrata a regime del sistema informaivo sanitario nazionale per verificarne gli effettivi risultati.

4.3 DANIMARCA

Nei Paesi del nord Europa (Danimarca, Finlandia, Islanda, Norvegia e Svezia), l'uso delle Tecnologie dell'Informazione e della Comunicazione nel settore pubblico, e, in particolare, in quello sanitario e dei servizi sociali, è ormai diffuso da diversi decenni; per tale ragione, la digitalizzazione dei summenzionati contesti ha, oggi, raggiunto, risultati maturi, al punto che, frequentemente ci si riferisce alle strategie, alle legislazioni, alle infrastrutture, e, più in generale, agli strumenti di *e-Health* adottati in questi Paesi parlando di eccellenza[147].

Con speciale attenzione alla Danimarca, l'interesse mostrato per lo scambio delle informazioni sanitarie in formato elettronico risale alla fine degli anni Ottanta, quando furono promosse iniziative specifiche negli ospedali di Vejle e Silkeborg per introdurre buone pratiche in questo settore; ulteriore progetto pioniere della comunicazione di dati medico-sanitari mediante lo *standard* "*Electronic Data Interchange*" fu quello realizzato ad Amager (1989-90) nel quale furono, invece, coinvolti farmacie e medici di medicina generale. A tutt'oggi, come indicato nella presentazione del progetto "*MedCom*", il sistema informativo sanitario danese utilizza le medesime piattaforme di comunicazione.

4.3.1 PROGETTO "*MEDCOM*"

Fondata nel 1994, "*MedCom - Det danske Sundhedsdatanet*[148]" è una *co-operative venture* tra enti pubblici, organizzazioni ed aziende private legate al settore sanitario danese[149]. Le prime iniziative ("*MedCom I*") furono realizzate dal 1994 al 1996; attualmente è in essere l'ottava edizione ("*MedCom VIII*", 2012-2013), dedicata al tema

[147] In proposito, di interesse lo studio NORDIC COUNCIL OF MINISTERS, *Health and Social Sectors with an "e". A study of the Nordic countries*, TemaNord 2005:531, 2005, Copenhagen, pp. 165.
[148] *The Danish Health Care Data Network*.
[149] Nel sito *web*, consultabile all'indirizzo http://www.medcom.dk/, sono disponibili i *deliverable* del Progetto e, nella sezione dedicata, i documenti ufficiali concernenti gli *standard* utilizzati.

"*Dissemination and technological future-proofing*". Per promuovere e diffondere in modo stabile i risultati ottenuti nelle fasi iniziali, con l'accordo finanziario tra le contee ed il governo centrale del 1999, fu, infatti, deciso di dare a tale realtà un assetto permanente. Nel corso del 2011 "*MedCom*" è diventato di proprietà del Ministero della Salute, delle regioni danesi e del governo locale della Danimarca, ricevendo da essi finanziamenti; il motivo principale di tale ampliamento risiede nel dare continuità agli obiettivi politici in tema di sanità elettronica e Fascicolo Sanitario Elettronico nonché nel fortificare la collaborazione clinica tra medici di base, ospedali pubblici e privati, laboratori, farmacie.
Scopo essenziale di "*MedCom*" fu sviluppare, a livello nazionale, *standard* di comunicazione per i messaggi clinici più comuni (lettere di dimissione ospedaliere, ordini dei *test* di laboratorio, "*ePrescription*", rimborsi da parte dell'assicurazione sanitaria pubblica etc.) scambiati, in lingua danese, tra ospedali pubblici, medici di medicina generale nonché aziende private legate al settore sanitario, come, ad esempio, le farmacie. Dopo un avvio piuttosto lento, la comunicazione dei documenti sanitari danesi avviene ormai, perlopiù, in formato elettronico; nuovo obiettivo fissato da "*MedCom*" per il 2012, è stata la digitalizzazione dei messaggi (tra cui lettere di dimissione e piani di assistenza a domicilio) inviati tra ospedali e casa di cura nei comuni.

"*The Danish Health Care Data Network*" è un "*logical data network*" che fin dai suoi esordi ha utilizzato "*Electronic Data Interchange*" (EDI), *standard* internazionale proposto dalle Nazioni Unite per l'interscambio cifrato dei dati elettronici[150]; in particolare, i messaggi si servono di "*Electronic Data Interchange For Administration, Commerce and Transport*" (EDIFACT), *standard* EDI, adottato anche da "*International Organization for Standardization*" (ISO 9735), grazie al quale è possibile trasferire automaticamente i dati (ad esempio quelli contenuti in una lettera di dimissioni ospedaliera) tra diversi sistemi informativi[151]. EDIFACT fornisce un insieme di regole sintattiche per la struttura dei dati, un protocollo per lo scambio interattivo delle informazioni (I-EDI), una standardizzazione dei messaggi per lo scambio tra una pluralità di soggetti (Paesi o aziende).
Dal 1994 ad oggi, "*MedCom*" ha messo a punto più di 60 diversi *standard*, disponibili sia nella versione EDIFACT sia nella versione OIO-XML, uno *standard* nazionale

[150] Il sito ufficiale de "*United Nations Economic Commission for Europe*" è disponibile all'indirizzo http://www.unece.org/trade/untdid/welcome.html.
[151] *The Danish Health Care Data Network* utilizza le seguenti tipologie di *standards* EDIFACT: "*Medical Service Request message*" (MEDREQ), "*Medical Service Report message*" (MEDRPT), "*Medical resource usage and cost message*" (MEDRUC), "*Discharge Summary Letter message*" (MEDDIS), MEDREF *for referrals*, CONTROL "*the acknowledgement message can be used to approve or reject a message or part of such and to acknowledge receipt of the message following a syntax check*".

perfezionato per la digitalizzazione del settore pubblico danese; obiettivo finale di "*MedCom*" è elaborare le nuove regole esclusivamente in OIO-XML[152].

Altro esito particolarmente importante, raggiunto da "*MedCom*" alla fine del 2003, è la realizzazione del Portale "*Sundhed.dk*"[153], il cui principale pilastro è proprio "*The Danish Health Care Data Network*"; analogamente al sistema informativo, le comunicazioni di dati con e dal Portale si basano sullo *standard* "*Electronic Data Interchange*". L'ampiezza e la complessità sottese a "*Sundhed.dk*" hanno orientato verso la predisposizione di varie fasi progettuali, il cui conseguimento è, al tempo stesso, risultato intermedio e finale dell'intera iniziativa.

Attraverso "*Sundhed.dk*" cittadini, pazienti ed operatori sanitari danesi possono accedere alle informazioni sanitarie di proprio interesse, quali, ad esempio, trattamenti ed appunti di cartelle cliniche, informazioni sulla medicina e sulle visite al medico di famiglia etc.; il cittadino può, altresì, conoscere i servizi erogati *online*, reperire ulteriori informazioni sul sistema sanitario (come tempi di attesa negli ospedali pubblici o valutazioni dei pazienti sulla qualità dei servizi) nonché creare reti con altri pazienti affetti dalla medesima patologia. Obiettivo principale del Portale è, inoltre, quello di creare un sistema di comunicazione solido per favorire l'interazione tra il paziente ed il medico.

4.4 ITALIA

Analogamente a quanto osservato per l'Austria, gli obiettivi indicati dalla Commissione europea ne "*e-Health Action Plan*" del 2004, orientati al miglioramento dei servizi sanitari nazionali attraverso l'uso delle nuove tecnologie digitali, spinsero l'Italia a porre in essere politiche ed azioni condivise per la pianificazione di un sistema nazionale di sanità elettronica, sicuro, affidabile e, al tempo stesso, volto all'interoperabilità. Il contesto del Paese appariva, infatti, caratterizzato da una forte disomogeneità, in parte conseguenza di un'inadeguata gestione della ripartizione di competenze tra Stato e Regioni in materia di assistenza sanitaria prevista dalla Costituzione italiana (*ex* art. 117)[154].

---

[152] Maggiori informazioni sul progetto "OIO-XML" sono consultabili nell'*homepage* del sito, raggiungibile all'indirizzo http://digitaliser.dk/.

[153] La *homepage* è consultabile all'indirizzo https://www.sundhed.dk/.

[154] A mero titolo esemplificativo si riportano alcune tra le iniziative più significative realizzate a livello territoriale per la digitalizzazione della cartella sanitaria personale: progetto "CRS-SISS" (Lombardia), progetto "SOLE, Sanità *On Line*" (Emilia Romagna), progetto "Conto Corrente Salute" (Liguria), progetto "Integrazione per l'Erogazione dei Servizi in Sanità - IESS" (Veneto/Trentino-Alto Adige), progetto "Libretto Sanitario Nazionale" (Veneto), progetto "Cartella Clinica del Cittadino - TreC" (Trentino-Alto Adige), progetto "Carta Sanitaria Elettronica" (Toscana), progetto "LUMIR" (Basilicata), progetto " Rete dei

Al fine, dunque, di armonizzare lo stato dell'arte e promuovere nuove iniziative condivise, nel 2005, fu istituito il "Tavolo permanente Sanità Elettronica", composto dai referenti del Dipartimento per la digitalizzazione della pubblica amministrazione e l'innovazione tecnologica della Presidenza del Consiglio dei Ministri, dai rappresentati del Ministero della Salute nonché dai rappresentanti nominati dai presidenti delle Amministrazioni Regionali e delle Province Autonome. Tre i livelli strategici individuati per dar vita ad un "insieme di sistemi informatici federati"[155]: la definizione di un patrimonio semantico comune ("Progetto Mattoni"[156]), l'implementazione del "Nuovo Sistema Informativo Sanitario" (NSIS)[157], la predisposizione di sistemi informativi sanitari locali operanti con l'infrastruttura nazionale. Scopi principali di un sistema informativo sanitario di tipo federato, nel quale, quindi, i dati sanitari rimangono di proprietà dell'ente che le ha generate, sono, da una parte, garantire l'affidabilità e la sicurezza delle informazioni scambiate, dall'altra, contenere l'impatto dei nuovi strumenti sulle infrastrutture territoriali esistenti.

Il "Piano di Sanità Elettronica" fu lo strumento operativo individuato per definire requisiti e *standard* della "Infrastruttura di Base per la Sanità Elettronica" (IBSE), sia per quanto concerne i processi tra sistemi ed attori, sia per quanto concerne gli oggetti informativi[158]. Le componenti dell'Infrastruttura di Base per la Sanità Elettronica sono raffigurabili su tre livelli: al primo, posto alla base del sistema informativo, sono collocati gli *standard* per l'interoperabilità individuati dal "Sistema Pubblico di Connettività e Cooperazione" (SPCoop)[159]; al secondo risiedono un "*InfoBroker Individuale Sanitario*" (IBIS) per realizzare un Fascicolo Sanitario Elettronico virtuale (referenziando i documenti individuali) nonché strumenti per facilitare l'interoperabilità sintattica/semantica; al terzo, gli *standard* per garantire l'integrità dei processi di collaborazione tra gli attori coinvolti.

Medici di Medicina Generale - MEDIR" (Sardegna). Una dettagliata descrizione dei progetti citati è riportata nel documento PROGETTO "INFRASTRUTTURA TECNOLOGICA DEL FASCICOLO SANITARIO ELETTRONICO" - INFSE, *Fotografia commentata sperimentazioni esistenti su FSE. eGov 2012 - Obiettivo Salute*, DEF, v. 1.5, Dicembre 2010, pp. 164, realizzato nell'ambito del progetto InFSE che verrà esaminato nel presente lavoro.

[155] *Cfr.* TAVOLO PERMANENTE SANITÀ ELETTRONICA DELLE REGIONI E DELLE PROVINCE AUTONOME, *Una politica per la sanità elettronica*, Note di riferimento per lo sviluppo della sanità elettronica, 2005, p. 6.

[156] Maggiori informazioni sul "Progetto Mattoni" (2003-2007) sono disponibili all'indirizzo http://www.mattoni.salute.gov.it/.

[157] Per approfondimenti si rinvia alla sezione del sito del Ministero della Salute dedicata al "Nuovo Sistema Informativo Sanitario", consultabile all'indirizzo http://www.nsis.salute.gov.it/.

[158] La strategia architetturale di riferimento per il sistema nazionale della Sanità Elettronica è illustrata in dettaglio nel documento TAVOLO DI LAVORO PERMANENTE SANITÀ ELETTRONICA DELLE REGIONI E DELLE PROVINCE AUTONOME, *Strategia architetturale per la Sanità Elettronica*, DEF, v. 01.00, 31.03.2006, pp. 56.

[159] Previsto dal decreto legislativo 28 febbraio 2005 n. 42, *Istituzione del sistema pubblico di connettività e della rete internazionale della pubblica amministrazione, a norma dell'articolo 10, della legge 29 luglio 2003, n. 229*, pubblicato in G.U. n. 73 del 30.3.2005. Ulteriori approfondimenti sul SPCC sono consultabili sul sito di "DigitPA", all'indirizzo http://www.digitpa.gov.it/spc.

Una posizione trasversale assumono, invece, le politiche di *privacy* e sicurezza nonché il *repository* contenente i modelli dei processi, dei servizi, dei dati (in termini di metadati) utilizzati nella "*Enterprise Architecture*" di tipo federato di IBSE. Peculiarità principale di IBSE è quella di essere stata ideata come infrastruttura del tutto decentralizzata rispetto alle realtà del Sistema Sanitario Nazionale, e ciò, sia per ridurre l'impatto sull'organizzazione di tali enti, sia per utilizzare il *know-how* e gli investimenti locali; il collegamento tra IBSE ed i sistemi informativi territoriali, avviene, pertanto, in modo non invasivo, attraverso "Porte di Dominio", le cui caratteristiche sono descritte nelle specifiche SPCoop.

Parallelamente alla definizione del "Piano di Sanità Elettronica", in quanto ad essa funzionale, fu, poi, la predisposizione di Piani di azione, nazionale e regionali, necessari per tradurre, in concrete azioni territoriali, le regole definite nel PSE.

In questo contesto, di altrettanta importanza è menzionare le "Linee guida nazionali per la realizzazione di un sistema di Fascicolo Sanitario Elettronico" del 2010, definite nell'ambito di un Tavolo interistituzionale, istituito nel 2008 dal Ministero della Salute e da esso coordinato, al quale hanno partecipato esperti dello stesso Ministero, rappresentanti delle Regioni designati dalla Commissione salute, del Dipartimento per la digitalizzazione della pubblica amministrazione e l'innovazione tecnologica della Presidenza del Consiglio dei Ministri, dell'ente per la digitalizzazione della Pubblica amministrazione "DigitPa" e dell'Autorità Garante per il trattamento dei dati personali (quest'ultima in qualità di osservatore)[160]. Scopo principale di questo documento programmatico è indicare gli elementi necessari ad una progettazione nazionale omogenea di Fascicolo Sanitario Elettronico, e ciò, soprattutto, considerata la molteplice varietà di progetti regionali esistenti, rispetto all'adozione di modelli architetturali, *standard* semantici, infrastrutture. In particolare, le "Linee guida" individuano i contenuti minimi da includere nella predisposizione del Fascicolo Sanitario Elettronico ("dati identificativi dell'assistito", "dati amministrativi relativi dell'assistenza", "documenti sanitari e socio-sanitari") e del *Patient Summary* ("intestazione", "dati essenziali", "altre informazioni sul paziente"), gli aspetti infrastrutturali da considerare (in particolare utilizzare un modello architetturale basato su *standard* aperti, scalabile, modulare, affidabile, integrato con il "Sistema Pubblico di Connettività e Cooperazione" etc.), gli *standard* tecnologici da adottare (orientamento espressamente rivolto a HL7 CDA rel. 2 per "*Patient Summery*" ed "*ePrescription*")

[160] Oggetto di Intesa da parte della Conferenza Stato-Regioni, le "Linee guida" sono state pubblicate in G. U. n. 50 del 2.3.2011.

nonché i livelli di sicurezza e di protezione dei dati da prevedere[161]. Di particolare interesse è, poi, l'attenzione rivolta per la "definizione di ruoli, profili, e modalità di accesso" al fine di garantire l'appropriatezza dell'uso dei dati personali dell'assistito, risultato, questo, ottenibile, anche attraverso la predisposizione di precise politiche di accesso ai dati per la gestione dei sistemi informativi sanitari.

4.4.1 PROGETTO "INFSE"

Il Progetto "Infrastruttura tecnologica del Fascicolo Sanitario Elettronico" (InFSE)[162], sorto nell'ambito di una collaborazione tra il Dipartimento per la digitalizzazione della pubblica amministrazione e l'innovazione tecnologica della Presidenza del Consiglio dei Ministri e il Dipartimento Tecnologie dell'Informazione e delle Comunicazioni[163] del Consiglio Nazionale delle Ricerche, è l'iniziativa nazionale, intrapresa nel 2010 ed oggi conclusa, per realizzare un modello architetturale per il Fascicolo Sanitario Elettronico, che garantisca la compatibilità con l'infrastruttura tecnologica in essere a livello territoriale nonché l'interoperabilità funzionale e semantica auspicata dalla Commissione europea e già oggetto dei progetti "IPSE" ed "*epSOS*"[164].

---

[161] Di questo profilo si darà conto nel capitolo dello studio dedicato al tema del trattamento e protezione dei dati personali.

[162] *Cfr.* PROGETTO "INFRASTRUTTURA TECNOLOGICA DEL FASCICOLO SANITARIO ELETTRONICO" - INFSE, *Infrastruttura tecnologica del Fascicolo Sanitario Elettronico. Linee guida eGov 2012 - Obiettivo Salute*, v. 1.2, Luglio 2012, pp. 135.

[163] Di cui fanno parte i seguenti Istituti: Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR), Istituto di Informatica e Telematica (IIT), Istituto di Scienza e Tecnologie dell'Informazione (ISTI) e Sistemi di Indicizzazione e Classificazione (URT DSP).

[164] Per implementare i risultati già ottenuti con il progetto "InFSE", a seguito di una nuova convenzione siglata, nel 2010, tra i medesimi soggetti (Dipartimento per la Digitalizzazione della Pubblica Amministrazione e l'Innovazione Tecnologica della Presidenza del Consiglio dei Ministri ed Dipartimento delle Tecnologie dell'Informazione e delle Comunicazioni del Consiglio Nazionale delle Ricerche), ha preso avvio il progetto "OpenInFSE - Realizzazione di un'infrastruttura operativa a supporto dell'interoperabilità delle soluzioni territoriali di fascicolo sanitario elettronico nel contesto del sistema pubblico di connettività". Obiettivi di questa nuova iniziativa (oggi è conclusa) sono stati: definire componenti *software* per l'interoperabilità del Fascicolo Sanitario Elettronico e, per la medesima finalità, realizzare un *network* interregionale, sviluppare modelli per l'integrazione di servizi per il cittadino (soprattutto alla luce della diffusione di *Personal Health Systems* per il monitoraggio remoto), promuovere azioni di raccordo con il progetto IPSE ed i progetti regionali implementati in tema di FSE (*cfr.* "*Allegato tecnico alla Convenzione per la realizzazione di un'infrastruttura operativa a supporto dell'interoperabilità delle soluzioni territoriali di fascicolo sanitario elettronico nel contesto del sistema pubblico di connettività*", consultabile all'indirizzo http://www.ehealth.icar.cnr.it/phocadownload/AllegatoTecnico.pdf.). A tal fine, sono state selezionate alcune realtà territoriali, quali Aziende Ospedaliere, Aziende Sanitarie Locali nonché i sistemi informativi territoriali di alcune Regioni e Province Autonome. I risultati, presentati nel luglio 2012, hanno mostrato che, utilizzando un'architettura analoga a quella delineata nel progetto InFSE è possibile ottenere sistemi interoperabili (a tal fine, le componenti software sviluppate nel Progetto OpenInFSE sono state integrate con i sistemi - eterogenei- di Fascicolo Sanitario Elettronico delle Regioni Calabria, Campania e Piemonte proprio utilizzando l'architettura InFSE). Ulteriore risultato raggiunto è stata l'interoperabilità di alcuni sistemi informativi regionali per lo scambio di *Patient Summary*, grazie all'utilizzo dell'infrastruttura proposta dal Progetto ("Registro Indice Federato" per la ricerca di documenti sanitari di un paziente contenuti nel dominio regionale; "Interfaccia di Accesso" e "Gestore dei Documenti" per il reperimento di uno

Tenendo conto della tipologia del sistema assistenziale italiano, l'architettura del Progetto "InFSE" prevede nodi regionali e locali ("completi" - se equivalenti a quelli regionali - o "assistiti"), che, avvalendosi del "Sistema Pubblico di Connettività", consentano le comunicazioni inter-regionali, per mezzo di "Porte di Dominio"[165]. Per raggiungere le summenzionate finalità, analogamente al Progetto *epSOS*, "InFSE" adotta una "*Service Oriented Architecture*" organizzata su tre livelli: "*Connectivity layer*" (la cui componente essenziale è il "Servizio Pubblico di Connettività"), "*Component layer*" (di cui fanno parte "Interfaccia di Accesso", "Gestore dei Documenti", "Registro Indice Federato", "Gestore delle Politiche di Accesso", "Gestore Gerarchico degli Eventi"), "*Business Layer*" ("*ePrescription*", "prenotazione visita specialistica", "ricovero")[166]. In questo scenario, una funzione centrale è affidata ai c.d. "attori", figure esterne all'Infrastruttura InFSE, chiamate, tuttavia, a svolgere precisi ruoli di interazione con il sistema informativo delineato.

Particolare attenzione è in questa sede rivolta al "*Component layer*", di cui, di seguito, si richiamano, alcuni elementi essenziali (sinteticamente rappresentati nella *figura 8*).

Figura 8 – "Component Layer" della SOA InFSE

specifico documento sanitario). In questo caso, le Regioni e Province Autonome coinvolte sono state le stesse che hanno preso parte al progetto IPSE. Ulteriori approfondimenti sul Progetto e sulle specifiche tecniche sono disponibili sul sito "*ICT&Health*", sezione "*OpenInFSE*", del Consiglio Nazionale Ricerche - Dipartimento delle Tecnologie dell'Informazione e delle Comunicazioni, consultabile all'indirizzo http://www.ehealth.icar.cnr.it/.

[165] Ivi, pp. 24-25.

[166] Ivi, p. 26.

L'"Interfaccia di Accesso"[167] è la componente che funge, sia a livello di nodo regionale sia a livello di nodo locale, da accesso all'infrastruttura del Fascicolo Sanitario Elettronico (esempî di interfacce sono "*IDocument*", "*IEvent*", "*IEntry*", "*IBrokerFederation*", "*IRegistryFederation*")[168], da parte degli attori coinvolti (quali, "*document consumer*", "*document producer*", "*event consumer*", "*event producer*" etc.); al tempo stesso essa svolge ulteriori funzioni, come da esempio, quelle di intercettare gli eventi occorsi.

Il "Registro Indice Federato"[169], composto appunto da più registri federati sincronizzati tra loro e sviluppati nel linguaggio "*ebXML*"[170], raccoglie le meta-informazioni dei documenti sanitari archiviati nei *repository* per facilitarne la ricerca e la memorizzazione; in taluni casi, esso ha la funzione di indice dei servizi, se, in particolare, raccogli metadati attraverso cui risalire ai servizi esposti dai nodi locali. Ogni regione può prevedere la presenza di più registri presso i nodi locali ("Registro locale"); ogni nodo regionale deve, invece, prevedere la presenza di almeno un "Registro regionale". Analogamente a quanto indicato per le "Interfacce di Accesso", anche in questo caso la tipologia di attori coinvolti è plurima (quali, "*Entry Producer*", "*Entry Consumer*", "*Registry Node*"), così come diverse sono le interfacce che il "Registro Indice Federato" deve supportare (ad esempio, "*IEventMgt*", "*IMetadataMgt*", "*IQueryMgt*", "*IRegistryFederationMgt*")[171].

Il "Gestore Gerarchico degli Eventi"[172] effettua il *routing* e la notifica degli eventi agli interessati; il modello adottato è il *publish/subscribe* basato su *broker*. La federazione di *broker* locali permette non soltanto di effettuare ricerche più efficaci a livelli decentrato, ma anche di consentire agli utenti di accedere al sistema attraverso qualsiasi *broker*. Per una più efficace gestione, tutti gli eventi sono classificati secondo un modello gerarchico. Attori di questa componente sono, ad esempio, "*Publisher*", "*NotificationProducer*",

---

[167] Ivi, pp. 27-59.

[168] In InFSE, le interfacce delle varie componenti adottano il linguaggio "*Web Services Description Language*" (WSDL), basato su XML ed utilizzato per descrivere le interfacce pubbliche dei Web Services e le modalità per accedere ad essi. Le specifiche delle interfacce di riferimento per l'implementazione dell'Infrastruttura tecnologica del Fascicolo Sanitario Elettronico sono riportate in PROGETTO "INFRASTRUTTURA TECNOLOGICA DEL FASCICOLO SANITARIO ELETTRONICO" - INFSE, *Specifiche delle interfacce. eGov 2012 - Obiettivo Salute*, v. 1.2, Luglio 2012, pp. 51.

[169] PROGETTO "INFRASTRUTTURA TECNOLOGICA DEL FASCICOLO SANITARIO ELETTRONICO" - INFSE, *Infrastruttura tecnologica del Fascicolo Sanitario Elettronico, cit.*, pp. 60-79.

[170] Una descrizione analitica del profilo di interoperabilità della componente "Registro Indice Federato" (conforme alle specifiche "*ebXML Registry Repository*") è contenuta in PROGETTO "INFRASTRUTTURA TECNOLOGICA DEL FASCICOLO SANITARIO ELETTRONICO" - INFSE, *Modello informativo dei metadati. eGov 2012 - Obiettivo Salute*, v. 1.2, Luglio 2012, pp. 71.

[171] *Cfr.* PROGETTO "INFRASTRUTTURA TECNOLOGICA DEL FASCICOLO SANITARIO ELETTRONICO" - INFSE, *Specifiche delle interfacce. eGov 2012 - Obiettivo Salute*, v. 1.2, Luglio 2012, pp. 51.

[172] PROGETTO "INFRASTRUTTURA TECNOLOGICA DEL FASCICOLO SANITARIO ELETTRONICO" - INFSE, *Infrastruttura tecnologica del Fascicolo Sanitario Elettronico, cit.*, pp. 80-106.

"*NotificationConsumer*"; interfacce del servizio "*IPublisherRegistrationgMgt*", "*ISubscriptionMgt*", "*INotificationBrokerMgt*", "*IBrokerFederationMgt*"[173].

Il "Gestore dei Documenti"[174] memorizza, in modo affidabile e non ripudiabile, in *repository* locali o regionali, i documenti sanitari contenenti tutti gli eventi relativi ad un paziente, documenti creati esclusivamente da utenti autorizzati[175]. Attori di questa componente sono "*DocumentProducer*" e "*DocumentConsumer*"; interfaccia del servizio è "*IDocumentMgt*"[176].

Il "Gestore delle Politiche di Accesso"[177] è il "*Component layer*" responsabile di tutti i profili di sicurezza, sia dei servizi infrastrutturali sia di quelli applicativi.

Affinché i dati sanitari di un assistito siano correttamente fruibili dai soggetti autorizzati alla loro consultazione, è indispensabile, non soltanto definire *policy* stringenti per i singoli sistemi, ma anche prevedere adeguati meccanismi di sicurezza. Per il raggiungimento di questo risultato, analogamente a quanto già illustrato in proposito del Progetto *ELGA*, "InFSE" utilizza tre funzioni - "Autenticazione", "Identificazione" e "Autorizzazione" -, avvalendosi dell'architettura di riferimento prevista dallo *standard* "*eXtensible Access Control Markup Language*"[178], linguaggio adottato per esprimere politiche di sicurezza per il controllo degli accessi, e del modello "*Role-Based Access Control*" (RBAC)[179]. La creazione di regole (*rule*) relative alle politiche di accesso - regole composte da *target*, effetto o decisione nonché condizione -, è strumentale alla conoscenza dei risultati dell'applicazione di una regola ad una *policy*, possibile grazie alla combinazione di algoritmi contenuti in un *dataset* predefinito. Attraverso tale meccanismo è, dunque, possibile conoscere se il soggetto richiedente (che svolge il ruolo "*x*"), sia o meno autorizzabile all'accesso ai dati.

---

[173] Ivi.
[174] Ivi, pp. 107-112.
[175] Per facilitarne l'interoperabilità, è preferibilmente che i documenti sanitari prodotti all'interno del sistema informativo sanitario siano strutturati secondo lo *standard* HL7 CDA rel. 2.0.
[176] PROGETTO "INFRASTRUTTURA TECNOLOGICA DEL FASCICOLO SANITARIO ELETTRONICO" - INFSE, *Specifiche delle interfacce, cit.*
[177] Il paradigma seguito in InFSE è "*Security As a Service*", adottato nelle *Service Oriented Architectures* per l'implementazione di un *Single Sign-On*.
[178] Come già indicato nella descrizione del progetto ELGA, l'architettura di riferimento XACML prevede le seguenti componenti: "*Policy Enforcement Point*" (PEP), "*Policy Information Point*" (PIP), "*Policy Decision Point*" (PDP), "*Policy Administration Point*" (PAP). Come segnalato dagli stessi promotori del Progetto, in InFSE ulteriori importanti riflessioni meritano gli aspetti semantici dei ruoli e quelli dichiarativi delle regole.
[179] Il modello RBAC prevede la gestione del controllo degli accessi in un sistema informativo basato sul ruolo; questo consente di restringere l'accesso alle informazioni, consentito esclusivamente agli utenti autorizzati.

La fase di "Autentificazione" precede le altre ed ha essenzialmente lo scopo di verificare l'identità degli utenti (fruitore ed erogatore del servizio), attraverso l'utilizzo di strumenti c.d. "forti", quali, ad esempio *smart card* di tipo CNS o CSE ("Carta Sanità Elettronica").
La fase di "Identificazione" è, invece, finalizzata a confermare l'identità dell'utente, che sarà, di conseguenza, abilitato all'esercizio delle azioni consentite; per creare un vero e proprio "portafoglio di asserzioni" utilizzabile nella fase successiva, il fruitore si serve delle seguenti componenti "*Profile Authority*" (PA)[180], "*Identity Provider*" (IdP)[181], "*Attribute Authority*" (AA)[182].
Infine, il processo di "Autorizzazione", strumento per verificare i diritti degli utenti che richiedono di poter consultare i dati sanitari (e ciò dal momento che non tutti gli utenti che posso accedere al Fascicolo Sanitario Elettronico godono dei medesimi diritti) e, al tempo stesso, per controllare gli accessi alle informazioni (sulla base del modello RBAC), intercettando, così, eventuali frodi.
Strumentali a tale processo sono le componenti architetturali di XACML, "*Policy Enforcement Point*", "*Policy Decision Point*", "*Policy Information Point*" e "*Policy Administration Point*", di cui si è già parlato illustrando il Progetto *ELGA*[183].

4.4.1.1 PROGETTO "OPENINFSE"

Il Progetto "OpenInFSE: realizzazione di un'infrastruttura operativa a supporto dell'interoperabilità delle soluzioni territoriali di fascicolo sanitario elettronico nel contesto del sistema pubblico di connettività", ad oggi concluso, si colloca nel contesto della Convezione siglata nel maggio 2009 tra il Dipartimento per la digitalizzazione della pubblica amministrazione e l'innovazione tecnologica della Presidenza del Consiglio ed il Dipartimento delle Tecnologie dell'Informazione e delle Comunicazioni del Consiglio Nazionale delle Ricerche per l'individuazione dell'architettura e delle specifiche tecniche idonee a rendere il FSE interoperabile a livello nazionale, senza al contempo ignorare lo

[180] "E' l'entità incaricata della gestione e manutenzione dei profili utente e può essere interrogata anche remotamente; il profilo è composto da n-ple strutturate, ad esempio, nel seguente modo: Nome Attributo, Valore Attributo, Riferimento logico dell'Authority in grado di validare l'attributo", in PROGETTO "INFRASTRUTTURA TECNOLOGICA DEL FASCICOLO SANITARIO ELETTRONICO" - INFSE, *cit*., p 119.
[181] "E' l'entità incaricata della gestione delle regole di identificazione. Si occupa dell'identificazione ed è innanzitutto un *Security Token Service* con il compito di generare, validare e rinnovare i *token* di sicurezza; si occupa altresì di interrogare gli AA per ottenere tutti gli attributi da inserire nella asserzione", in *ibidem*.
[182] "E' l'entità atta a gestire le informazioni sugli operatori, gli assistiti e le loro correlazioni temporali; si identifica con i basamenti e viene interrogata mediante un'operazione di *AttributeQuery*; sulla base degli attributi necessari per la fase di autorizzazione presenti nell'elemento *AttributeConsumingService* dei propri metadati, fornisce come risposta una asserzione SAML con i valori degli attributi richiesti", in *ibidem*.
[183] PROGETTO "INFRASTRUTTURA TECNOLOGICA DEL FASCICOLO SANITARIO ELETTRONICO" - INFSE, *Infrastruttura tecnologica del Fascicolo Sanitario Elettronico, cit.*, 113-134.

scenario europeo. Il Progetto si colloca, pertanto, in continuità con i risultati del Progetto "InFSE", di cui, appunto, ha fatto proprie le specifiche architetturali per la realizzazione del FSE (ad esempio, per ciò che concerne le interfacce "*Unified Model Language*" e "*Web Service Description Language*").

Scopi principali del Progetto "OpenInFSE" sono la realizzazione e lo sviluppo di componenti *software* per l'interoperabilità del FSE adottatte da aziende sanitarie e sistemi regionali (quali progettazione di *wrapper* per l'integrazione di FSE esistenti nelle Regioni e Province autonome partecipanti al Progetto[184] ed individuazione di un codice identificativo univoco dell'assistito) nonché la definizione di un vero e proprio *network* interregionale per l'interoperabilità delle soluzioni territoriali di FSE basato sui protocolli adottati nell'ambito del SPC (HL7, HL7-CDA2, XML etc). Secondo quanto indicato nell'Allegato tecnico del Progetto, ulteriore obiettivo di "OpenInFSE" è lo "sviluppo di modelli per l'integrazione di servizi a valore aggiunto per il cittadino", tra cui la progettazione di "servizi per l'acquisizione e la memorizzazione in tempo reale di data stream" e la "relizzazione di alcune componenti di base".

Centrale è, inoltre, la funzione che "OpenInFSE" svolge nel collegare le attività del progetto "IPSE - sperimentazione di un sistema per l'Interoperabilità europea e nazionale delle soluzioni di fascicolo sanitario elettronico: componenti Patient Summary ed Eprescription" e dei progetti regionali in tema di FSE.

4.4.1.2 PROGETTO "EVOLUZIONE E INTEROPERABILITÀ TECNOLOGICA DEL FASCICOLO SANITARIO ELETTRONICO"

Il Progetto "Evoluzione e interoperabilità tecnologica del Fascicolo Sanitario Elettronico", a tutt'oggi in essere, coinvolge i medesimi soggetti dei progetti "InFSE" e "OpenInFSE"; si colloca in continuità ripetto allo scenario rappresentato e, per alcuni profili, costuisce un ampliamento e consolidamento degli obiettivi perseguiti con i progetti già conclusi, tra cui, ad esempio rientrano l'implementazione dei moduli *software* dell'infrastruttura tecnologica del FSE nonché la definizione di modelli strutturati di dati clinici per l'interoperabilità semantica. Inoltre, particolarmente interessante è il *focus* sul *Cloud Computing* in sanità, in merito al quale il Progetto intende definire linee guida per lo sviluppo di servizi di Fascicolo Sanitario Elettronico su architetture *Cloud*.

[184] Lombardia, Abruzzo, Emilia Romagna, Molise, Friuli Venezia Giulia, Sardegna, Toscana, Umbria, Veneto e Provincia autonoma di Trento.

3.4.2 PROGETTO "IPSE"

Dall'Accordo di collaborazione interregionale sottoscritto, nel 2008, tra Ministero del Lavoro, della Salute e delle Politiche sociali - settore Salute, Ministero per la Pubblica Amministrazione e l'Innovazione, Regioni Lombardia (ente capofila), Abruzzo, Molise, Emilia Romagna, Toscana, Umbria, Veneto, Sardegna, Provincia Autonoma di Trento ed Agenzia Regionale della Sanità della Regione Autonoma Friuli Venezia Giulia, nel 2010 prese avvio il progetto "IPSE - sperimentazione di un sistema per l'Interoperabilità europea e nazionale delle soluzioni di fascicolo sanitario elettronico: componenti Patient Summary ed Eprescription" (IPSE), un'iniziativa nata come raccordo tra le soluzioni ideate a livello nazionale e quanto avviato con il Progetto *epSOS*[185].

Scopo principale del Progetto, conclusosi nel 2012, fu, dunque, la promozione dell'interoperabilità dei servizi di "*Patient Summary*" ed "*ePrescription*"[186].

In conformità con le indicazioni previste dal progetto *epSOS*, il collegamento tra i Paesi membri coinvolti avviene attraverso la rete *peer-to-peer* di "*National Contact Point*"; al "NCP" italiano al quale afferiscono le informazioni provenienti dalle Regioni. Nodo mediano, realizzato dal progetto "IPSE", tra il "NCP" ed i "*Regional Contact Point*" (cui spetta l'identificazione del cittadino e del tipo di richiesta) è un "*Italian Adapter*", attraverso cui, un cittadino italiano che si trovi per cure all'estero, può reperire i propri dati sanitari contenuti in "*Patient Summary*" e/o "*ePrescription*".

Per quanto concerne l'architettura tecnologica, il progetto "IPSE" utilizza le soluzioni suggerite ed intraprese dal Progetto "InFSE"; per quanto, invece, concerne la struttura dei documenti informatici, lo *standard* utilizzato è "*HL7 Clinical Document Architecture*".

[185] La *homepage* del Progetto è disponibile all'indirizzo http://ipse.cup2000.it/.

[186] *Workpackage* del progetto "IPSE" sono: WP 1, "analisi e confronto delle realizzazioni regionali su cooperazione e eHealth" (affidato alla regione Sardegna); WP 2, "analisi del contesto legale italiano" (coordinato dalla Toscana); WP 3, "definizione delle specifiche tecniche e dell'architettura di sistema" (gestito dal Friuli Venezia Giulia); WP 4"realizzazione dei Siti Pilota" (affidato alla regione Emilia Romagna); WP 5, "coordinamento e disseminazione" (assegnato alla Lombardia).

CAPITOLO III

SISTEMI INFORMATIVI E DATI PERSONALI IN SANITÀ ELETTRONICA

SOMMARIO: 1. "*Security*" e "*privacy*" tra sistemi informativi e diritti dell'utente - 2. Profili di sicurezza dei sistemi informativi - 2.1 Cenni su Sistemi di Gestione della Sicurezza delle Informazioni e *standard* di sicurezza informatica - 2.1.1 Sicurezza informatica in sanità - 3. Introduzione al tema della "*privacy*". Uno sguardo ai principi giuridici comunitari - 3.1 La direttiva 95/46/CE - 4. I dati sanitari nelle Raccomandazioni del Consiglio d'Europa - 5. Il trattamento dei dati sanitari in Italia - 5.1 La disciplina dei dati sanitari nel "Codice in materia di protezione dei dati personali" - 5.2 Le "Linee guida in tema di fascicolo sanitario elettronico e di *dossier* sanitario" del Garante per la protezione dei dati personali - 5.3 "Il Fascicolo Sanitario Elettronico. Linee guida nazionali" del Ministro della Salute - 5.4 La recente normativa nazionali in materia di sanità digitale e Fascicolo Sanitario Elettronico – 5.4.1 I decreti-legge 179/2012 e 69/2013 - 5.4.2 Lo schema di decreto sul Fascicolo Sanitario Elettronico attualmente all'esame della Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e Bolzano

1. "*SECURITY*" E "*PRIVACY*" TRA SISTEMI INFORMATIVI E DIRITTI DELL'UTENTE

Attori, ruoli, transazioni, dati, sono alcune significative parole-chiave che identificano le dinamiche dei Sistemi Informativi Sanitari, strumenti automatizzati, appositamente creati per la gestione dei flussi informativi prodotti dalle singole organizzazioni aziendali e dal sistema sanitario nel suo insieme. In particolare, "processi" (direzionali, gestionali ed operativi), "basi di dati" e "*Data Base Management System*" contribuiscono ad ottimizzare l'impiego delle risorse investite e consentono la comunicazione delle informazioni associate alle attività clinico-diagnostiche grazie all'utilizzo di *dataset* condivisi. Oltre alla funzione assunta dalle numerose componenti tecniche dei sistemi informatici (come *repository*, *server*, *gateway*, *secure node*)[187], di non secondaria importanza è il ruolo svolto da tutte le persone fisiche (tra essi, pazienti e familiari; soggetti operanti all'interno degli organigrammi aziendali - come *manager* e personale amministrativo, operatori sanitari e para-sanitari, ricercatori clinici etc. - nonchè *stakeholder* e *policymaker*) a vari livelli parte delle dinamiche socio-assistenziali.

[187] Per ulteriori approfondimenti sui profili tecnici si rinvia a INTEGRATING THE HEALTHCARE ENTERPRISE, *IHE IT Infrastructure (ITI), Technical Framework*, Volume 1 (ITI TF-1), Integration Profiles, Revision 9.0 - Final Text, August 31, 2012, p. 9.

Tutti i summenzionati attori sono titolari, benché con accezioni diverse, di informazioni sensibili, passibili di minacce esterne[188], che meritano, dunque, protezione, sia per motivi di *business*, nel caso delle aziende sanitarie, sia per la salvaguardia di un diritto fondamentale, nel caso degli utenti/pazienti. Per assicurare l'integrità, la riservatezza e la disponibilità dei dati personali, nella prassi sono stati sviluppati *standard* di sicurezza informatica e norme legislative *ad hoc* (*cfr. fig. 9*).

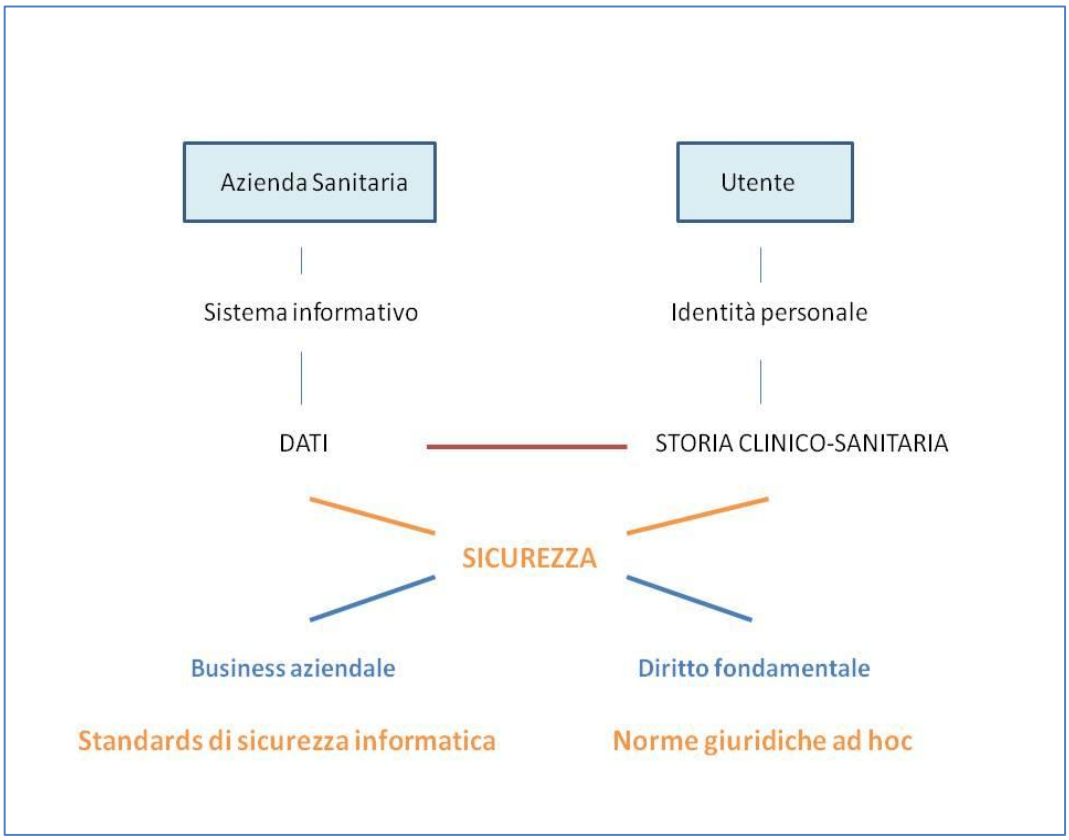


Figura 9 - La tutela dei dati sensibili

Quanto premesso introduce l'idea fondamentale a partire da cui si sviluppa il presente capitolo: sicurezza dei sistemi informativi sanitari e protezione dei dati personali sono due aspetti distinti ma complementari, e ciò, dal momento che, scopo della loro implementazione è la salvaguardia di un interesse, inerente ora una persona fisica (o "*user*") ora un sistema (*cfr. fig. 10*). Senza l'utilizzo di tecnologie per la sicurezza, sarebbe difficile, se non impossibile, fornire dispositivi adeguati a proteggere e tutelare dati appartenenti ad individui, società ed organizzazioni; inoltre, proprio la disponibilità di forti

[188] Gli attacchi ai sistemi o alle reti possono essere più o meno strutturati ed essere causati da "*virus*", "*worm*", "*intruder*" (come "*hacker*"), "*insider*", "*information warfar*" condotte da Paesi terzi, organizzazioni criminali o terroristiche.

tecnologie per la sicurezza induce i consumatori a rilasciare il proprio consenso per la raccolta e la memorizzazione delle informazioni sensibili.

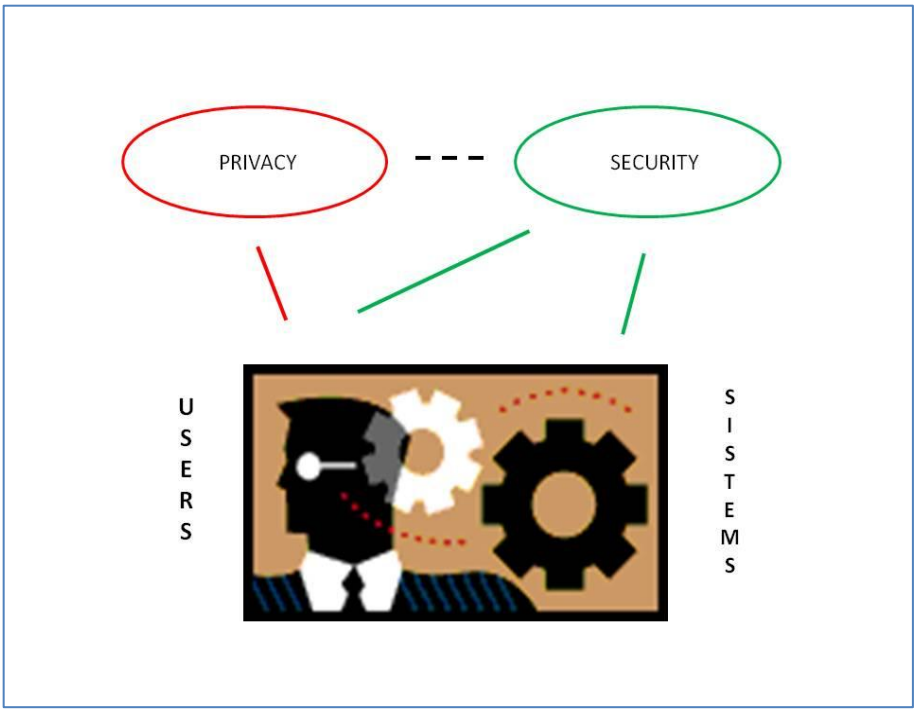


Figura 10 - *Privacy:Security=User:System*

É, comunque, essenziale chiarire cosa s'intende con i termini "*security*" e "*privacy*", evitando l'errore del comune sentire di considerarli impropriamente sinonimi; infatti, sebbene i due concetti siano alla base della progettazione delle Tecnologie dell'Informazione e della Comunicazione, essi indicano idee, e quindi strumenti, differenti e non interscambiabili. Se, infatti, la sicurezza è funzionale alla protezione dei dati personali, tuttavia, sistemi informativi sicuri possono non rispettare del tutto le norme in materia di *privacy*, e, addirittura, in taluni casi, esservi in conflitto[189].

2. PROFILI DI SICUREZZA DEI SISTEMI INFORMATIVI

Scopo sostanziale della sicurezza informatica (o "*computer security*") è la tutela di dati e sistemi di elaborazione (*network* o *personal computer*), attraverso la disposizione di programmi e dispositivi *hardware*. Principio cardine di tale disciplina è, dunque, la riservatezza delle informazioni ("*confidentiality*"), prevalentemente garantita attraverso la

[189] J.L. FERNÁNDEZ-ALEMÁN ET AL., *Security and privacy in electronic health records: A systematic literature review*, Journal of Biomedical Informatics (2013), [in press], http://dx.doi.org/10.1016/j.jbi.2012.12.003; B. BLOBEL, P. PHAROW, *Analysys and Evaluation of EHR Architecture*, Method Inf. Med. 2/2009, pp. 162-169.

prevenzione di accessi non autorizzati ai sistemi informativi. A tal fine sono definiti regole e strumenti che accertino l'identità degli utenti ("*authentication*") ed assicurino l'integrità dei dati ("*integrity*"), la cui modifica o cancellazione è prerogativa dei soli soggetti autorizzati; altrettanto significative sono, in tal senso, le misure per verificare la paternità dei messaggi inviati ("*non repudiation*") e controllare il corretto funzionamento dei sistemi, tenendo traccia di tutte le azioni intercorse ("*auditability*"). Parimenti centrale è poi permettere, ai soli utenti abilitati, di utilizzare, nei tempi e modi previsti, i sistemi informativi ("*availability*")[190].

La progettazione di sistemi sicuri passa, in primo luogo, attraverso un'effettiva conoscenza della loro struttura e delle possibili problematiche sottese; un approccio di tal genere può, infatti, favorire la predisposizione di modelli architetturali e tecnologie che, con maggiore efficacia, rispondano ai livelli di sicurezza previsti dalle norme esistenti. Occorre, ad esempio, tener conto delle modalità di diffusione dei dati (reperibili in *databases*, *file systems*, documenti elettronici), della natura delle Reti (siano esse aziendali o globali), dei requisiti minimi di sicurezza per l'accesso ai sistemi da parte degli utenti (come modalità di identificazione e di autenticazione); essenziale è, inoltre, pianificare gestione e controllo delle infrastrutture (predisponendo strumenti idonei, come "*log management*" e "*change and configuration management*") nonché regolamentare forme, efficienti ed efficaci, per la valutazione dei processi ("*auditing*") e della conformità alle procedure e alle norme delineate ("*compliance*").

Secondo alcuni autori, dal punto di vista operativo la "*computer security*" segue l'equazione "*Protection = Prevention + (Detection + Response)*"[191], ove per prevenzione ("*prevention*") s'intende l'insieme delle misure volte al controllo degli accessi[192]; per rilevazione ("*detection*"), la predisposizione di strumenti come "*audit log*", "*intrusion detection system*", "*honeypot*"[193]; per risposta ("*response*"), la messa in atto di procedure di

[190] Per quanto concerne il panorama italiano, tutti i summenzionati principi sono disciplinati dal d. lgs. 30 giugno 2003 n. 196, *Codice in materia di protezione dei dati personali*, pubblicato in G.U. n. 174 del 29.07.2003 - S.O. n. 123.

[191] Così in WM. A. CONKLIN, G. WHITE, *Principles of Computer Security. CompTIA Security+™ and Beyond*, The United States of America, Mc Graw Hill, Second edition, pp. 22-23.

[192] Sono esempi di contollo degli accessi *router, firewall, authentication hardware and software, encryption, intrusion detection system*.

[193] Il "registro di controllo" (o "*audit log*") è lo strumento utilizzato per il monitoraggio delle informazioni temporali rilevanti per un certo oggetto; per "*intrusion detection system*" s'intende, invece, un dispositivo che permette di identificare accessi non autorizzati ai computers o alle reti locali, ed, in particolare, di rilevare eventuali attacchi alle reti informatiche. In sicurezza informatica il concetto di "*honeypot*" rinvia ad un sistema (può trattarsi di un *computer*, un *file*, un *record* etc.) usato per tendere un vero e proprio tranello a quanti sono interessati ad informazioni riservate dell'azienda ed alle quali non sono autorizzati ad accedere.

"*backup*", "*computer forensics*", o la consultazione di "*incident response team*"[194]. Tecniche e strumenti che rendano effettiva la sicurezza, attiva e passiva, delle informazioni "sensibili" o, comunque riservate, sono, pertanto, fondamentali.

Quanto premesso sottolinea un altro importante aspetto: la sicurezza è una strategia omnicomprensiva e, in un certo senso, strutturale per ogni azienda. Pertanto, essa richiede, *in primis*, una riflessione attenta sulle dinamiche attive e passive connesse al tema in esame e, conseguentemente, la predisposizione di mezzi idonei a monitorare l'intero *iter* dei dati, del quale fanno parte la fase di generazione così come quelle di memorizzazione e riuso; la conoscenza di possibili minacce e reati è, altresì, essenziale per operare secondo criteri e modalità efficienti ed efficaci, che salvaguardino l'interesse del singolo (persona fisica o giuridica) e della collettività[195].

Nello scenario sanitario, proprio per la natura dei dati trattati e per il numero di processi ed attori coinvolti, la programmazione di sistemi informativi sicuri è centrale, sia dal punto di vista dei sistemi stessi sia dal punto di vista degli utenti. Infatti, se, da una parte, per rilasciare il proprio consenso al trattamento dei dati personali, i pazienti necessitano di elevate garanzie di affidabilità dei sistemi, al tempo stesso, per utilizzare in modo adeguato i Fascicoli Sanitari Elettronici, il personale sanitario richiede idonee rassicurazioni

---

[194] La "copia di sicurezza" (o "*backup*") è il procedimento di sovente adottato per conservare dati ed informazioni su supporti informatici diversi dalla memoria di massa del computer. Il termine "*computer forensics*" indica, in generale, la disciplina che si occupa della individuazione, conservazione, protezione, estrazione, documentazione, impiego e trattamento del dato informatico oggetto di valutazione di un processo giuridico (*cfr.* A. PHILIPP, D. COWEN, C. DAVIS, *Hacking Exposed: Computer Forensics*, second edition, McGraw Hill, 2009, pp. 544). Per risolvere i problemi dovuti ad incidenti informatici, spesso conseguenza della vulnerabilità dei *softwares*, sono identificati appositi gruppi di esperti, noti come "*incident response team*", le cui conoscenze e competenze sono a servizio della sicurezza informatica dei sistemi.

[195] Nella prassi sono stati definiti alcuni criteri per la predisposizione di *software* idonei a rendere *computer system* e *network* sicuri; tali indirizzi sono prevalentemente ispirati ai seguenti "modelli": "*confidentiality model*" e "*integrity model*".

Al primo "modello" ("*confidentiality model*"), fa, ad esempio, riferimento "*The Bell-LaPadula security model*", elaborato agli inizi degli anni Settanta ed il cui scopo è evitare il danneggiamento, deliberato o accidentale, delle informazioni da parte di individui non autorizzati a riceverle. A tal fine, "*The Bell-LaPadula security model*" segue due regole: (i) "*Simple Security Rule*", secondo cui per poter accedere alle informazioni occorre un'autorizzazione di livello inferiore a quella del documento di interesse e (ii) "*-*property*", secondo cui un soggetto può scrivere in un oggetto/*file* solo se la classificazione del suo livello di sicurezza è inferiore o uguale alla classificazione dell'oggetto.

Al secondo modello ("*integrity model*") sono, invece, ispirati "*The Biba Security Model*", risalente alla fine degli anni Settanta, e "*The Clark-Wilson Security Model*". La visione sottesa a "*The Biba Security Model*" è opposta rispetto a quella di cui a "*The Bell-LaPadula security model*"; principi cardine de "*The Biba Security Model*" sono infatti: (i) "*Low-Water-Mark policy*", secondo cui un soggetto può eseguire un programma solo se il livello di integrità del programma è uguale o inferiore al livello di integrità del soggetto e (ii) "*Ring policy*", principio in base al quale qualsiasi soggetto è autorizzato alla lettura di qualsiasi oggetto senza necessità di verificare alcun livello di integrità dell'oggetto stesso. A differenza di tutti i precedenti modelli citati, "*The Clark-Wilson Security Model*" è stato disegnato per limitare i processi; in quest'ottica, un individuo può modificare i dati solo attraverso specifici "*Trasformation processes*" ben identificati.

Per ulteriori approfondimenti si rinvia a: WM. A. CONKLIN, G. WHITE, *Principles of Computer Security. CompTIA Security+™ and Beyond*, The United States of America, Mc Graw Hill, Second edition, pp. 42-45.

soprattutto in termini di responsabilità professionale che, ad esempio, possono sorgere a seguito di manomissioni dei meccanismi di identificazione o autenticazione.

Come evidenziato in premessa, l'interazione tra attori e sistemi informativi è essenzialmente centrata sull'identità e sui ruoli svolti dagli stessi: affinché i dati possano essere consultabili dai soggetti interessati e, quindi, sia di fatto garantita la loro protezione, è, anzitutto, indispensabile verificare l'identità del richiedente ("*identification*") ed il tipo di autorizzazione o permesso rilasciato per l'accesso ai dati ("*authentication*"); solo nel caso in cui i due processi - di identificazione e di autenticazione[196] - siano positivamente conclusi, la consultazione delle informazioni sanitarie sarà autorizzata ("*authorization*"). Infine, durante la fase di "*access control*" è accertato in quali sistemi, risorse o applicazioni un soggetto (*user* o *computer system*) può effettivamente entrare.

Svariate sono le modalità per compiere i suddetti controlli; tra quelli già menzionati nel capitolo precedente rientrano "*Role-Based Access Control*" (RBAC)[197] e "*Rule-Based Access Control*" (RBAC). Peculiarità comune è il fatto che la validità dell'accesso non si basa sul permesso rilasciato ad un soggetto per consultare un determinato oggetto: nel primo caso, infatti, essa si fonda sulla gamma di ruoli ritenuti abilitanti e ricoperti proprio da quel soggetto, nel secondo sull'insieme di regole che definiscono i parametri di accessibilità.

Oltre a "*Role-Based Access Control*" e "*Rule-Based Access Control*", altri metodi per il controllo degli accessi sono "*Discretionary Access Control*" (in questo caso il criterio utilizzato per limitare l'accesso ad un oggetto è basato sull'identità di un soggetto e/o di un gruppo di provenienza; la discrezionalità si fonda sul fatto che il soggetto può trasferire il permesso di accesso a terzi, anche senza particolari controlli, a meno che non ne sia stato imposto espresso divieto) e "*Mandatory Access Control*" (la limitazione di accesso ad un oggetto è, invece, basata sulla "sensibilità" dell'informazione contenuta in un oggetto - "*Top Secret*", "*Secret*" etc. -; in particolare, è il sistema operativo, e non il soggetto, a determinare in quali casi l'accesso è permesso a terzi).

---

[196] Comuni metodi utilizzati per i processi di identificazione ed autenticazione sono l'uso di ID (o *username*) e *password*; carte magnetiche contenenti informazioni personali; sistemi di riconoscimento biometrico; certificati e firme digitali; *tokens*; *Single Sign-on*.

[197] Il RBAC, divenuto nel 2004 come ANSI/INCITS *standard*, fu per la prima volta formalizzato in D. F. FERRAIOLO, D. R. KUHN, *Role-Based Access Controls*, 15th National Computer Security Conference (1992), Baltimore MD, pp. 554-563. Il modello fu integrato nel 2000 (R. SANDHU, D. FERRAIOLO, R. KUHN, *The NIST Model for Role-Based Access Control: Towards A Unified Standard*, Proceedings of the fifth ACM workshop on Role-based access control, 2000, pp. 46-63), con il *framework* definito nello studio R. S. SANDHU, E. J. COYNEK, H. L. FEINSTEINK, C. E. YOUMAN, *Role-Based Access Control Models*, IEEE Computer, Vol. 29, N. 2, February 1996, pp. 38-47.

Per attuare sistemi informativi sicuri e gestire le dinamiche sottese alla sicurezza dei sistemi stessi, le organizzazioni aziendali predispongono anche *policy*, procedure, *standard* e linee guida. Le prime identificano principi e risultati auspicati e, pur non entrando nei dettagli operativi, hanno un valore imperativo; le seconde prescrivono, invece, in modo particolareggiato, le azioni da porre in essere per il raggiungimento degli obiettivi aziendali; gli *standard* prevedono indicazioni tassative per l'implementazione delle *policy*; le linee guida, infine, raccolgono raccomandazioni relative alle *policy* stesse.

Per le finalità di questo studio particolare attenzione meritano le "*security policy*", nelle quali l'azienda definisce non soltanto il concetto di sicurezza che all'interno del proprio sistema ha valore, ma anche gli obiettivi perseguiti e gli strumenti utilizzati per implementare ambienti operativi sicuri.

Nelle "*security policy*" sono previste le risorse utili per la produttività delle *performance* aziendali nonché le attività permesse e negate per tale scopo (c.d. "*Acceptable Use Policy*"); regolati gli usi di Internet all'interno dell'azienda (o "*Internet Usage Policy*") nonché la tipologia di messaggi che i lavoratori possono inviare "da" e "con" gli strumenti informatici aziendali, sia per proteggere la sicurezza dei sistemi sia per mantenere elevato il rendimento professionale del personale occupato (c.d. "*E-Mail Usage Policy*"); indicate le disposizioni per regolare le modalità di gestione dei dati con particolare riferimento ai profili di protezione e sicurezza ("*Due Care and Due Diligence*").

In termini di "*security policy*" è egualmente importante che siano individuati criteri e procedure per la definizione di *password* da parte degli utenti (ad esempio indicando un numero minimo di caratteri da scegliere, la frequenza di aggiornamento, la distribuzione etc.) (c.d. "*Password Management*"); regolate le modalità di protezione delle informazioni (quali soggetti possono avervi accesso, chi ha l'autorità di rilasciarle e secondo quali criteri e forme, i metodi di distruzione delle stesse etc.) (si parla, in questo caso di "*Classification of Information*"); definite le regole per la soppressione dei dispositivi elettronici contenenti informazioni e dati aziendali (o "*Disposal and Destruction*"); previste adeguate strategie in caso di modifiche delle infrastrutture IT (ad esempio per ciò che riguarda l'aggiornamento delle prassi aziendali, i dispositivi *software* e *hardware*, la ricognizione delle infrastrutture etc.) (c.d. "*Change Management Policy*").

Nelle "*security policy*" rientra, inoltre, la suddivisione di compiti e poteri in materia di sicurezza tra le figure aziendali designate, e ciò, dal momento che la cooperazione tra i soggetti responsabili è essenziale per il buon fine delle transazioni, soprattutto perché consente di evitare forme di accentramento di potere (profilo noto anche come "*Separtion*

of Duty"); parimenti centrale è, infine, la divulgazione minima di informazioni all'interno del contesto aziendale, divulgazione che, comunque, deve esclusivamente avvenire per finalità operative ed ai soli soggetti coinvolti nei procedimenti di interesse (principio conosciuto come "*Need to Know and Least Privilege*").

2.1 Cenni su Sistemi di Gestione della Sicurezza delle Informazioni e *standard* di sicurezza informatica

Salvaguardare integrità, riservatezza e disponibilità dei dati raccolti nei sistemi informativi, limitando, quindi, minacce e rischi di attacchi informatici, è uno dei motivi principali per cui le aziende, di cui quelle sanitarie rappresentano un campione cospicuo sul fronte pubblico nazionale, implementano sistemi di gestione della sicurezza delle informazioni (o "*Information Security Management System*"); beneficiari dell'adozione di tali strumenti sono prevalentemente gli stessi enti, che, grazie al controllo dei flussi informativi, possono accrescere le proprie *performance* e strategie di *marketing*. Per quanto, invece, concerne gli utenti, in generale, essi traggono vantaggio dalla sicurezza dei sistemi soltanto in modo indiretto[198]; una delle rilevanti differenze tra l'adozione di strumenti a tutela della "*security*" e della "*privacy*" consiste, infatti, proprio in questo: la tipologia di dati protetti è, nel primo caso, riferita alla società, nel secondo, al singolo individuo.

Quanto evidenziato avvalora la tesi della complementarietà tra le misure in esame (già sinteticamente introdotta in *figura 2*) nonché l'importanza di adottare un approccio olistico nella definizione teorica delle stesse, approccio, peraltro, egualmente assunto nel *design* degli strumenti di *Information and Communication Technology*.

La complessità e la trasversalità del dominio in esame hanno richiesto agli esperti un impegno esclusivo, volto a considerare, non soltanto i profili più propriamente tecnologici della sicurezza delle informazioni, ma anche quelli organizzativi e procedurali, di cui, a titolo esemplificativo, valutazione e gestione del rischio figurano come problemi emergenti e prioritari.

Per ottemperare alle summenzionate esigenze, e, in particolare, per implementare sistemi di gestione della sicurezza delle informazioni uniformi, sono stati predisposti gli *standard* internazionali di sicurezza informatica, di cui la famiglia ISO/IEC 27000,

[198] A titolo esemplificativo, la predisposizione di buone misure di sicurezza può contenere, fino ad annullare, i casi di c.d. "furto d'identità", come il "*phishing*".

sviluppata da "*International Organization for Standardization*" - "*Joint Technical Committee Information Technology*", è un significativo esempio[199].

Ai fini del presente studio è rilevante menzionare: ISO/IEC 27001:2005, "*Information security management systems - Requirements*", norma che specifica i requisiti (soprattutto in termini di sicurezza fisica, organizzativa e logica) per attuare, rendere operativo, monitorare, revisionare, mantenere e migliorare un sistema di gestione della sicurezza delle informazioni; ISO/IEC 27002:2005, "*Code of practice for information security management*", vere e proprie linee guida e principi generali per l'avvio, l'implementazione, la gestione ed il miglioramento della sicurezza delle informazioni di un'organizzazione, in linea con lo *standard* ISO/IEC 27001:2005[200]; ISO/IEC 27006:2011, "*Requirements for bodies providing audit and certification of information security management systems*", in cui sono identificati gli *standard* per la certificazione degli *audits*. Inoltre, in riferimento al tema in esame, parimenti rilevanti sono: ISO/IEC TR 13335-1:1996, "*Guidelines for the management of IT Security - Part 1: Concepts and models for IT Security*", norma dedicata alla gestione della sicurezza informatica, nonché gli *standard* ISO/IEC 15408:2008 (*part 1*, *2* e *3*)[201], noti anche come "*Common Criteria*", le cui indicazioni permettono di testare le applicazioni aziendali per renderle conformi agli *standard* vigenti in materia di sicurezza.

2.1.1 SICUREZZA INFORMATICA IN SANITÀ

Analogamente a quanto riferito per la sicurezza informatica, anche il tema della sicurezza informatica in sanità è oggetto di crescente interesse da parte della comunità

---

[199] Gli *standard* della famiglia ISO/IEC 27000 sono stati elaborati dalla sotto-commissione 27 "*IT Security Techniques*", *Working Group* 1 "*Information security management systems*". Altri *Working Group* (WG) della JTC 1/SC 27 sono: WG 2 "*Cryptography and security mechanisms*", WG 3, "*Security evaluation, testing and specification*", WG 4 "*Security controls and services*", WG 5, "*Identity management and privacy technologies*". Gli *standards* della famiglia ISO/IEC 27000 sono consultabili nella "Appendice", cui si rinvia.

[200] Già ISO 17799:2005, la norma ISO/IEC 27002:2005 deriva dallo *standard* "BS 7799-1", pubblicato nel 1995 dal BSI (*British Standards Institute*) ed ora ritirato. Al "BS 7799-1" si affiancava il "BS 7799-2", a sua volta sostituito dallo *standard* ISO/IEC 27001:2005.

Aree tematiche di cui ISO/IEC 27002:2005 espressamente si occupa sono: politiche di sicurezza; sicurezza organizzativa; gestione del risparmio; sicurezza del personale; sicurezza fisica e ambientale; gestione di comunicazioni e operazioni; controllo degli accessi; acquisizione, sviluppo e manutenzione dei sistemi informativi; informazioni di sicurezza per la gestione degli incidenti; *business continuity management*; conformità.

[201] In dettaglio trattasi di ISO/IEC 15408-1:2008 "*Evaluation criteria for IT security - Part 1: Introduction and general model*", ISO/IEC 15408-2:2008 "*Evaluation criteria for IT security - Part 2: Security functional components*" e ISO/IEC 15408-3:2008 "*Evaluation criteria for IT security - Part 3: Security assurance components*".

scientifica[202]: il rapido diffondersi dei recenti strumenti digitali, come Fascicoli Sanitari Elettronici e *Personal Health Device*, ha posto in luce, infatti, nuove problematiche connesse alla maggiore, e talora più facile, accessibilità ad informazioni e dati sensibili da parte di soggetti non autorizzati; in questo scenario, non sono poi mancate specifiche iniziative giuridiche, sia a livello europeo sia a livello nazionale. Nel corso degli ultimi anni, i mutati approcci hanno, altresì, determinato una significativa svolta nel ruolo dei sistemi informativi sanitari, principalmente legata ai fattori contingenti già esaminati nei primi due capitoli del presente studio. In particolare, la definizione di *standard* tecnologici, la previsione di sistemi *hardware* e *software* uniformi, l'introduzione di politiche volte all'interoperabilità, la previsione di nuove *governance* orientate alla sicurezza, l'*empowerment* dei pazienti, sono solo alcune delle cause che hanno contribuito ad un ripensamento dell'organizzazione e della struttura dei sistemi tradizionali nei quali, invece, prevalevano dinamiche (locali e non) integrate nonché funzioni perlopiù di tipo operativo, non collegate, quindi, a strategie o programmazioni socio-sanitarie. Sebbene tutti gli operatori e gli utenti di questo settore abbiano un'elevata consapevolezza del fatto che proteggere, in modo assoluto, i dati informatizzati non sia possibile, sono, però, egualmente forti la volontà e l'esigenza di ridurre al minimo i danni conseguenti da accessi impropri ai dati sensibili. Al fine di sopperire a tali esigenze, sono state, ad esempio, elaborate specifiche tecniche di de-personalizzazione e de-identificazione per rendere anonimi i dati contenuti nei Fascicoli Sanitari Elettronici; predisposti strumenti per crittografare i dati sensibili trasmessi tramite Internet; implementate tecnologie di "*Radio Frequency IDentification*" (RFID) per l'identificazione e la tracciabilità dei dati sanitari[203].

L'attenzione rivolta all'interoperabilità dei sistemi informativi sanitari risveglia ed acuisce, inoltre, l'intenzione di realizzare mezzi digitali sempre più sicuri, e ciò, soprattutto perché, in uno spazio distribuito più che nei sistemi centralizzati, maggiori sono i rischi da considerare, ad esempio, in termini di integrità, scambio, memorizzazione dei dati nonché responsabilità, civile e penale, delle figure designate.

Congiuntamente ad un profondo processo di riforma culturale che riguardi tutti i soggetti, a qualsiasi titolo coinvolti nello sviluppo, implementazione e fruizione degli

[202] Tra gli altri, si rinvia a: R.J. ANDERSON, *Security in Clinical Information Systems*, University of Cambridge, 1996; E. SMITH, J.H.P. ELOFF, *Security in health-care information systems-current trends*, International Journal of Medical Informatics 54 (1999), pp. 39-54; D. GRITZALISA, C. LAMBRINOUDAKIS, *A security architecture for interconnecting health information systems*, International Journal of Medical Informatics (2004) 73, pp. 305-309, B. THURAISINGHAM, *Security standards for the semantic web*, Computer Standards & Interfaces 27 (2005), pp. 257-268.

[203] Tra gli altri, *cfr*. A. BUSCEMI, A. CARRARO, *L'innovazione tecnologica RFID a garanzia della sicurezza del paziente*, in Diritto Sanitario Moderno, 2011, 59, pp. 1-12.

strumenti di sanità elettronica, l'attività di standardizzazione rappresenta, almeno in linea teorica, un importante pilastro: l'adozione di modelli condivisi può agevolare la diffusione di *best practice* sia a livello sovranazionale sia a livello nazionale e locale. Anche in questo caso, per molteplici ragioni, beneficiari finali sono gli *stakeholder* direttamente ed indirettamente interessati ai processi di diagnosi e cura.

Con specifico riferimento ai Sistemi di Gestione della Sicurezza delle Informazioni nel settore della sanità elettronica, analogamente a quanto più in generale era stato disposto con lo *standard* ISO/IEC 27002:2005, la "*Technical Committee Health Informatics*" di "*International Organization for Standardization*" ha elaborato la norma ISO 27799:2008, "*Information security management in health using ISO/IEC 27002 (TC 215)*", il cui scopo è la formalizzazione di vere e proprie linee guida e principi generali per l'avvio, l'implementazione, la gestione ed il miglioramento della sicurezza delle informazioni nelle organizzazioni sanitarie.

Per quanto, infine, concerne i Fascicoli Sanitari Elettronici, peculiari "*security standard*" sono: ISO/TS 13606-4:2009, "*Electronic health record communication - Part 4: Security*", norma che definisce metodologia e requisiti di sicurezza generale applicabili alle comunicazioni tra EHRs; ISO/TS 22600-1:2006, "*Privilege management and access control - Part 1: Overview and policy management*", *standard* per la condivisione di informazioni tra fornitori non affiliati alla sanità, organizzazioni sanitarie, compagnie di assicurazione sanitaria, pazienti, personale e *partner* commerciali; ISO/TS 14265:2011, "*Classification of purposes for processing personal health information*", in cui sono classificate le finalità per cui le informazioni sanitarie personali possono essere elaborate, a supporto di una gestione coerente delle informazioni nella fornitura di servizi di assistenza sanitaria e per la comunicazione di cartelle cliniche elettroniche attraverso i confini organizzativi e giurisdizionali.

3. INTRODUZIONE AL TEMA DELLA "*PRIVACY*". UNO SGUARDO AI PRINCIPI GIURIDICI COMUNITARI

Il concetto di "*privacy*" richiede alcune osservazioni preliminari, dal momento che nella dottrina giuridica e nella giurisprudenza italiane, così come nella normativa comunitaria e nazionale, la definizione di questo diritto fondamentale è stata, ed è a tutt'oggi, oggetto di numerosi interventi e dibattiti[204]. L'attualità della suddetta tematica è particolarmente

[204] Significativo lo studio ARTICLE 29 WORKING PARTY ON DATA PROTECTION, *Thirteenth Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data and*

legata alla diffusione delle Tecnologie dell'Informazione e della Comunicazione, che, se da una parte consentono la semplificazione dei processi aziendali ed amministrativi, dall'altra non sono scevre di pericoli: le informazioni del singolo, di frequente utilizzate da enti pubblici e privati per molteplici finalità, sono, infatti, talora, esposte ad azioni illegittime da parte di terzi; per ovviare a tali conseguenze è essenziale predisporre strumenti, di prevenzione e di protezione, che rendano efficace la tutela diretta della sfera individuale (secondo quanto già, peraltro, illustrato in *figura 10*).

Originariamente indicata da Warren e Brandeis come "*the right to be let alone*"[205] e, successivamente, da Westin come "*the claim of individuals, groups, or institutions, to determine when, how, and to what extend information about them is communicated to others*"[206], negli anni Novanta la "*privacy*" è stata definita da Rodotà come "diritto di mantenere il controllo sulle proprie informazioni e di *determinare le modalità di costruzione della propria sfera privata*. L'oggetto di questo diritto si specifica […] - secondo l'insigne giurista - nel 'patrimonio informativo attuale o potenziale' di un soggetto"[207]. La posizione di Rodotà coglie due dimensioni essenziali di questo diritto fondamentale: da una parte la riservatezza (con cui molte volte il termine "*privacy*" è, di fatto, esclusivamente assimilato nel contesto giuridico e, più in generale, nel contesto culturale italiano), dall'altra l'identità personale[208].

La suddetta lettura è, peraltro, in linea con quanto previsto dal quadro normativo europeo: già affermata dall'articolo 8 della "Convenzione europea dei diritti dell'uomo"[209], la "protezione dei dati di carattere personale" trova un ulteriore importante riconoscimento transnazionale nell'articolo 8 della "Carta dei diritti fondamentali dell'Unione europea", ai

---

privacy in the European Union and in third countries covering the year 2009 - adopted on 14 July 2010, Brussels, 2011, pp. 132; altrettanto interessanti i risultati de GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Relazione 2010. Evoluzione tecnologica e protezione dei dati*, 2010, pp. 320.

[205] Vedasi: S. WARREN, L. BRANDEIS, *The Right to Privacy*, in Harvard Law Review, 4, 1890, pp. 193-220.

[206] *Cfr*. A. WESTIN, *Privacy and Freedom*, Bodley Head, 1967, pp. 487.

[207] Così in S. RODOTÀ, *Privacy e costruzione della sfera privata* (1991), in Id., Tecnologie e diritti, Bologna, Il Mulino, 1995, pp. 101-122.

[208] Secondo quanto, in modo peraltro del tutto condivisibile, è stato osservato in G. PINO, *Teorie e dottrine dei diritti della personalità Uno studio di meta-giurisprudenza analitica*, in "Materiali per una storia della cultura giuridica", 2003/1, pp. 237-274.

[209] Rubricato "Diritto al rispetto della vita privata e familiare", l'articolo 8 della CEDU così recita: "1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui". La "*Convenzione europea dei diritti dell'uomo*", firmata a Roma il 4 novembre 1950 ed entrata in vigore il 3 settembre 1953 (modificata ed integrata da 14 "Protocolli aggiuntivi"), è oggi stata ratificata da tutti i 47 Stati membri del Consiglio d'Europa.

sensi del quale: "1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente"[210].

Le norme invocate richiamano molti dei principi già ricordati nei paragrafi dedicati al tema della sicurezza dei sistemi informativi, e ciò proprio a dimostrazione della reciproca funzionalità tra i due aspetti qui esaminati; a titolo esemplificativo, l'identificazione del soggetto, l'accessibilità dei dati, il rilascio di consenso cui è subordinato il trattamento, sono elementi strutturali per il *design* dei sistemi informativi così come per la predisposizione di regolamenti aziendali e normative nazionali.

3.1 LA DIRETTIVA 95/46/CE

Importante pietra miliare del diritto comunitario in materia di "tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" è la direttiva 95/46/CE, che, per la sua stessa natura giuridica, ha vincolato gli Stati membri a prevedere forme e mezzi adeguati al raggiungimento dei risultati indicati[211].

A tutt'oggi in essere, la Direttiva è articolata in otto capi, contenenti 34 articoli; le definizioni di "dati personali" e "trattamento di dati personali" sono previste nel capo I dedicato alle "disposizioni generali".

---

[210] *Cfr. Carta dei diritti fondamentali dell'Unione europea* (2010/C 83/02), pubblicata in Gazzetta ufficiale dell'Unione europea C 83/389 del 30.3.2010.

[211] *Cfr. Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, pubblicata in G.U. n. L 281 del 23.11.1995. Fanno parte del quadro giuridico comunitario in materia di protezione dei dati personali anche la *Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)*, pubblicata in G.U. L 201 del 31.7.2002, il *Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati*, pubblicato in G.U. L 008 del 12.01.2001 nonché la *Direttiva 1999/93/CE del Parlamento europeo e del Consiglio del 13 dicembre 1999 relativa ad un quadro comunitario per le firme elettroniche*, pubblicata in G.U. L. 13 del 13.12.1999.
Per ulteriori approfondimenti sulle implicazioni della direttiva europea sulla protezione dei dati personali, di interesse: M. D. BIRNHACK, *The EU Data Protection Directive: An engine of a global regime*, Computer Law&Security Report, 24 (2008) 508-520.

In particolare, ai sensi dell'articolo 2, comma I, lettera a), per "dati personali" s'intende "qualsiasi informazione concernente una persona fisica identificata o identificabile"[212]; fin dall'*incipit* dell'articolato normativo emerge la volontà del legislatore europeo, volontà peraltro riconoscibile già nell'articolo 1, di preferire una nozione ampia di "dati personali", consentendo così all'interprete di riconoscere e tutelare i diritti individuali in un numero cospicuo di casi[213]. Interessante, infatti, notare che la nozione di "dati personali" è comprensiva sia delle fattispecie in cui, per un terzo soggetto, è possibile identificare direttamente il titolare delle informazioni (ad esempio perché sono noti estremi anagrafici, dati biometrici, ma anche indirizzi IP, attività di *browsing*, *login*, liste di siti *web* visitati), sia di quelle in cui ciò avviene in modo indiretto (trattasi dei casi in cui la presenza di precisi parametri permette di risalire, in modo univoco ed inequivocabile, ad una persona, circostanza, questa, frequentemente riscontrabile nei *database* dedicati ad una specifica rilevazione di informazioni, in cui, oltre al dato di interesse, sono altresì collezionate indicazioni che inevitabilmente fanno convergere verso lo stesso soggetto, come data di nascita, numero di documento, codice di avviamento postale etc.)[214].

Il concetto di "trattamento di dati personali", di cui alla lettera b) dell'articolo 2, comma I, fa, invece, riferimento a "qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione"[215]. Centrale è, in questo senso, la garanzia di "anonimia" dei dati personali raccolti, possibile attraverso meccanismi di de-identificazione delle informazioni (a titolo esemplificativo, la data di nascita, convertita in

[212] Il comma primo, lettera a), dell'articolo 2, prosegue chiarendo che: "si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale".

[213] Particolarmente interessante il documento ARTICOLO 29 GRUPPO DI LAVORO PER LA PROTEZIONE DEI DATI PERSONALI, *Parere 4/2007 sul concetto di dati personali - adottato il 20 giugno*, 01248/07/IT, WP 136, pp. 27, in cui "Articolo 29. Gruppo di lavoro per la protezione dei dati personali" ha formulato orientamenti su come interpretare, e applicare il concetto di dati personali ai sensi della direttiva 95/46/CE e della legislazione comunitaria correlata.

[214] Importante, altresì, ricordare che identificativi Internet, come indirizzi IP, attività di *browsing* di un utente, *login*, liste dei siti *web* visitati dall'utente etc. sono parametri classificati come dati personali.

[215] *Cfr. Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, pubblicata in Gazzetta ufficiale n. L 281 del 23.11.1995.

una "categoria di età" rende più difficile il collegamento diretto o indiretto all'utente in questione).

La manifestazione esplicita ed inequivocabile di consenso del consumatore[216], l'obbligo di informativa da parte del responsabile del trattamento o suo rappresentante, il diritto di accesso ai dati da parte della persona interessata nonché la rettifica, la cancellazione o il congelamento di dati incompleti o inesatti, i principi di riservatezza e sicurezza tecnica e di organizzazione dei sistemi sono, tra gli altri, previsti nel capo II, dedicato alle "condizioni generali di liceità dei trattamenti di dati personali".

Ai fini del presente studio, di altrettanto interesse è quanto disposto dall'articolo 17, norma già richiamata nel capitolo I in quanto presupposto della Comunicazione del 2007 della Commissione al Parlamento europeo e al Consiglio sulla protezione dei dati personali attraverso l'utilizzo delle *Privacy Enhancing Technology*.

In particolare, il primo comma dell'articolo 17 sancisce: "gli Stati membri dispongono che il responsabile del trattamento deve attuare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali. Tali misure devono garantire, tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere".

Security policy, strategie per la pianificazione ed implementazione di *best practice* aziendali orientate alla protezione dei sistemi, organizzazione degli ambienti di lavoro e degli assetti amministrativi, gestione delle infrastrutture IT, controllo degli accessi e delle modalità di trasmissione dei dati in Rete, modalità di conservazione e distruzione dei dati, sono solo alcuni dei casi che rientrano nella norma in esame.

Il capo III della direttiva in esame contiene, invece, la disciplina in tema di "ricorsi giurisdizionali, responsabilità e sanzioni" per violazione dei diritti. Particolarmente significativa è l'attenzione del legislatore comunitario per gli "adeguati livelli di garanzia" da prevedere a protezione dei dati personali, anche nei casi di trattamento all'estero (profilo disciplinato nel capo IV, titolato "trasferimento di dati personali verso paesi terzi").

[216] Per approfondimenti si rinvia a ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 15/2011 on the definition of consent - Adopted on 13 July*, 201101197/11/EN, WP187, pp. 38.

I capi V e VI sono rispettivamente dedicati a "codici di condotta" e "autorità di controllo e gruppo per la tutela delle persone con riguardo al trattamento dei dati personali"; organo consultivo europeo indipendente, istituito dall'articolo 29, "*the Article 29 Data Protection Working Party*" si occupa di osservare, riferire e raccomandare in merito ai livelli di "*privacy*" esistenti sia all'interno della Comunità europea sia nei paesi terzi. Rilevante, in proposito, ricordare gli impulsi forniti dal "Gruppo di lavoro" alle autorità nazionali garanti per la protezione dei dati personali anche sul tema della tutela delle informazioni sensibili in sanità[217].

La direttiva 95/46/CE si conclude con il capo VIII, "misure comunitarie di esecuzione", e le "disposizioni finali" in cui la Commissione riconosce la necessità di possibili ulteriori interventi sul "trattamento dei dati sotto forma di suoni o immagini relativi a persone fisiche" proprio per il ruolo che le nuove tecnologie stanno assumendo (così, in particolare, raccomanda l'articolo 33).

Dall'analisi svolta si evince l'importanza della centralità della tutela dei dati personali; tale realtà, tuttavia, non va letta in modo isolato, bensì connessa con un altro fondamentale diritto di "prima generazione": la libertà dell'individuo. Porre in essere azioni e politiche volte a prevenire i rischi legati al mancato o inadeguato trattamento delle informazioni sensibili consente, infatti, di preservare la libertà del cittadino nelle sue molteplici espressioni, imperativo questo piuttosto rilevante nella "società dell'informazione", in cui le minacce di violazione per il singolo e, in un certo senso, per la stessa collettività, sono elevate. La natura che i dati personali, ed in particolare i c.d. dati "sensibili" (tipologia di informazioni di cui fanno parte anche quelle idonee a rivelare lo stato di salute), rivestono, richiede, però, una regolamentazione ed un trattamento *ad hoc*, funzionali a tutelarne caratteristiche ed interessi.

L'esame del quadro giuridico europeo in materia di protezione dei dati personali non sarebbe completo se si ignorasse un rilevante e recente intervento del Parlamento europeo e del Consiglio: la proposta di un regolamento generale sulla protezione dei dati presentata il 25 gennaio 2012[218] e già definita nella Comunicazione della Commissione

[217] I compiti del "Gruppo" sono, altresì, stabiliti dall'articolo 15 della direttiva 2002/58/CE. Ulteriori informazioni sull'attività ed i documenti prodotti da "*the Article 29 Data Protection Working Party*" sono consultabili all'indirizzo http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.

[218] Trattasi di COMMISSIONE EUROPEA, *Proposta di Regolamento del parlamento europeo e del consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)*, Bruxelles, 25.1.2012, COM(2012) 11 def. Contestualmente, per la revisione del quadro giuridico in materia di *privacy*, è stato presentato un altro documento, e, precisamente, COMMISSIONE EUROPEA, *Proposta di Direttiva del parlamento europeo e del consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da*

"*Salvaguardare la privacy in un mondo interconnesso. Un quadro europeo della protezione dei dati per il XXI secolo*"[219].

Le ragioni che hanno orientato gli organi comunitari verso questa proposta di revisione dell'apparato giuridico in materia di *privacy* sono principalmente da rintracciare nelle nuove modalità di utilizzo dei dati attraverso le TIC. Rispetto al secolo scorso, infatti, i limiti di condivisione e raccolta delle informazioni sono mutati; l'assenza di norme chiare sulla protezione dei dati personali può rappresentare un significativo deterrente per i consumatori che si trovano ad operare nell'ambiente digitale. Le "nuove sfide" orientano verso la definizione di una politica forte e coerente in materia di protezione dei dati personali nonché la predisposizione di un quadro giuridico più solido e "globale", considerata la frammentarietà delle legislazioni vigenti all'interno dell'Unione europea[220].

Di notevole interesse per il presente lavoro, anche alla luce delle considerazioni che verranno espresse nei paragrafi seguenti, l'incoraggiamento della Commissione verso l'utilizzo di strumenti che rafforzino la sicurezza dei dati; indicativo, in proposito, il disposto di cui all'articolo 23 della proposta di regolamento, rubricato "Protezione fin dalla progettazione e protezione di default". La *ratio iuris* va individuata in un principio di garanzia della protezione dei dati personali fin da una fase progettuale delle procedure e dei sistemi di trattamento delle informazioni da parte del responsabile del trattamento[221].

4. I DATI SANITARI NELLE RACCOMANDAZIONI DEL CONSIGLIO D'EUROPA

L'*excursus* dei provvedimenti comunitari e nazionali (vincolanti e non, di rango primario e secondario) rivela una pressoché omogenea convergenza sul concetto di "dati sanitari", genericamente intesi come informazioni relative allo stato di salute di una persona[222], la cui ulteriore declinazione rimane, però, affidata all'interprete. In proposito, è

---

parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati, Bruxelles, 25.1.2012 COM(2012) 10 def.

[219] COMMISSIONE EUROPEA, *Comunicazione della Commissione al parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Salvaguardare la privacy in un mondo interconnesso. Un quadro europeo della protezione dei dati per il XXI secolo*, Bruxelles, 25.1.2012, COM(2012) 9 def.

Per approfondimenti sul tema ivi introdotto, di interesse ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 08/2012 providing further input on the data protection reform discussions*, WP199, 01574/12/EN, Brussel, 2012, pp.45.

[220] COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, Un approccio globale alla protezione dei dati personali nell'Unione europea*, Bruxelles, 4.11.2010, COM(2010) 609 def.

[221] *Cfr.* Appendice.

[222] Oltre alle informazioni che in modo più intuitivo fanno parte di questa categoria (in quanto specifici di un singolo soggetto), altri significativi esempi di "dati sanitari" sono: buone pratiche sanitarie, Fascicoli Sanitari

necessario un avvertimento: come accade in tutte le discipline giuridiche, l'eccessivo spazio lasciato agli operatori del diritto, ora conseguenza dell'assenza di norme ora conseguenza di una disordinata iperproduttività normativa, non produce alcun effetto positivo né sul fronte teorico né su quello applicativo; creare apparati sistematici è, dunque, di centrale interesse sia per i tecnici sia per beneficiari delle norme vigenti, particolarmente in un settore multidisciplinare come quello dell'*e-Health*.

Un documento significativo sulla tematica in esame è la "Raccomandazione n. R (97) 5 del Comitato dei Ministri agli Stati membri relativa alla protezione dei dati sanitari"[223], con cui il Consiglio d'Europa ha appunto sollecitato i legislatori nazionali a tradurre i principi affermati in atti giuridici di diritto interno. Cuore della Raccomandazione sono le modalità di raccolta e trattamento automatizzato dei dati sanitari nonché la salvaguardia del carattere riservato e della sicurezza dei dati personali relativi alla salute.

Richiamando l'articolo 6 della "Convenzione per la protezione delle persone in materia di trattamento automatizzato dei dati personali"[224], ai sensi del quale i dati personali sulla salute non possono essere trattati automaticamente a meno che il diritto interno non preveda garanzie appropriate, il Consiglio d'Europa ravvisa la necessità di rivedere quanto affermato, negli anni Ottanta, nella "Raccomandazione n. R (81) 1 relativa alla regolamentazione applicabile alle banche di dati sanitari automatizzate"[225], e ciò, soprattutto a seguito dei progressi determinati dall'applicazione delle Tecnologie dell'Informazione e Comunicazione anche al settore sanitario.

Nello scenario rappresentato dalla Raccomandazione del 1997, il rispetto della vita privata è ancora una volta riconosciuto come diritto fondamentale da salvaguardare durante ogni attività di raccolta e trattamento dei dati personali; a tal fine, ad esempio, è indispensabile che i soggetti titolari del trattamento siano professionisti sanitari o, comunque, persone/organismi che agiscono per conto di operatori sanitari qualificati.

Garanzie parimenti importanti sono l'utilizzo di mezzi leciti e leali nel trattamento delle informazioni concernenti lo stato di salute di un paziente nonché l'identificazione,

---

Elettronici nel loro insieme, immagini diagnostiche, dati molecolari, genetici ed epigenetici, proteomici e metabolici, informazioni sulle campagne di vaccinazione, sugli stili di vita della popolazione, sull'ambiente e sui costumi, dati sociali etc.

[223] CONSIGLIO D'EUROPA - COMITATO DEI MINISTRI, *Raccomandazione n. R (97) 5 del Comitato dei Ministri agli Stati membri relativa alla protezione dei dati sanitari*, adottata dal Comitato dei Ministri il 13 febbraio 1997.

[224] *Cfr*. CONSIGLIO D'EUROPA, *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*, Strasburgo, 28 gennaio 1981.

[225] *Cfr*. CONSIGLIO D'EUROPA - COMITATO DEI MINISTRI, *Raccomandazione n. R (81) 1 del Comitato dei Ministri agli Stati membri relativa alla regolamentazione applicabile alle banche di dati sanitari automatizzate*, adottata dal Comitato dei Ministri il 23 gennaio 1981.

puntualmente disciplinata dal diritto interno, delle specifiche finalità per le quali i dati sanitari sono utilizzati.

In questo contesto si colloca, inoltre, l'obbligo di informativa alla persona interessata, informativa che deve vertere su: (i) l'esistenza di un archivio, (ii) le finalità della raccolta dei dati, (iii) i soggetti autorizzati a compierla, (iv) la possibilità di rifiutare o ritrattare il consenso prestato e le relative conseguenze, (v) il responsabile dell'archiviazione. Uniche deroghe di informativa ammissibili sono i) per prevenire un pericolo concreto o reprimere una infrazione penale, ii) per ragioni di salute pubblica, iii) a protezione della persona interessata e dei diritti e libertà altrui, iv) in caso di urgenza medica[226].

Altrettanto centrali sono il consenso (informato, autonomo, specifico) dell'interessato al trattamento dei dati sanitari; la riservatezza nella comunicazione delle informazioni personali nonché il diritto di accesso ai dati personali e alla rettifica dei dati errati.

"Contro la distruzione - accidentale o illecita - e la perdita accidentale, così come contro l'accesso, la modificazione, la comunicazione o ogni altra forma di trattamento non autorizzati"[227] è, inoltre, indispensabile l'adozione di misure tecniche ed organizzative idonee alla protezione dei dati sanitari; a tal fine sono suggerite misure volte al "controllo all'entrata delle istallazioni", controllo dei supporti di dati, della memoria, dell'utilizzazione, ma anche controlli d'accesso, della comunicazione, dell'introduzione, del trasporto, nonché controllo di disponibilità delle stesse informazioni[228].

L'articolo 10 della Raccomandazione 97/5, rubricato "conservazione", indica come regola generale che la conservazione dei dati sanitari sia eguale alla "durata necessaria per raggiungere lo scopo per il quale essi sono stati raccolti e trattati"; la norma prevede anche la possibilità di cancellazione degli stessi dati, su istanza dell'interessato, "a meno che essi non siano resi anonimi o che non vi si oppongano interessi superiori e legittimi ed in particolare quelli enunciati al punto 10.2 [quali l'interesse legittimo della salute pubblica, della scienza medica, del responsabile del trattamento sanitario o del responsabile dell'archivio, al fine di permettergli di esercitare o di difendere i suoi diritti giuridici, o a fini storici o statistici], o obbligazioni di archiviazione".

La Raccomandazione in esame affronta, in conclusione, i temi dei "flussi transfrontalieri" e della "ricerca scientifica".

---

[226] Così precisa al punto 5.6 la *Raccomandazione n. R (97) 5 del Comitato dei Ministri agli Stati membri relativa alla protezione dei dati sanitari*.
[227] Secondo quanto si legge al punto 9.1 della stessa *Raccomandazione n. R (97) 5*.
[228] Ivi, punto 9.2.

Secondo quanto dettato dall'articolo 11, in linea generale sono negati i flussi di dati sanitari tra Stati che non assicurino una protezione conforme a quanto previsto dalla "Convenzione per la protezione delle persone nei confronti del trattamento automatizzato di dati a carattere personale" del Consiglio d'Europa, con la sola eccezione dei casi in cui siano adottate idonee misure di sicurezza e sia rilasciato il consenso dell'interessato.
Secondo quanto poi disposto dall'articolo 12, l'uso dei dati sensibili per finalità di ricerca scientifica è ammissibile purché avvenga in forma anonima e, ove ciò non sia possibile, purché sia oggetto di consenso informato per le finalità della ricerca, consenso che, quindi, non soltanto è obbligatorio, ma deve anche essere precedente al trattamento[229].

5. IL TRATTAMENTO DEI DATI SANITARI IN ITALIA

Come più volte evidenziato, l'evoluzione delle applicazioni di *Information and Communication Technology* in sanità ha, tra l'altro, determinato l'adozione di nuovi modelli organizzativi, il mutamento della fruibilità dei dati sanitari nonché la diffusione di forme digitali per la memorizzazione dei dati sensibili, che, dai faldoni cartacei, stanno rapidamente migrando verso supporti informatici[230]. I detti cambiamenti richiedono, però, una vera e propria armonizzazione multidisciplinare tra tecnologia, sanità e diritto; tuttavia, per le ragioni già illustrate nei capitoli precedenti, tale risultato, seppur su più fronti auspicato, si sta realizzando secondo velocità piuttosto eterogenee.

Con precisa attenzione alla compagine giuridica, non può, ad esempio, non constatarsi che tra le cause concorrenti all'arretratezza del sistema rientrano la farraginosità e la lentezza del processo legislativo italiano.
Principale conseguenza di questo stato dell'arte è il *vacuum legis*, che, ha indotto, tra il 2009 ed il 2010, autorità amministrative, come Ministero della Salute ed Autorità garante per la protezione dei dati personali, a predisporre atti idonei ad introdurre principi in tema di *e-Health* nonché indicazioni per la risoluzione di fattispecie concrete.
La suddetta regolamentazione ha investito anche il Fascicolo Sanitario Elettronico, strumento che, se dal punto di vista tecnico-sanitario è oggetto di progetti ed iniziative in essere, dal punto di vista normativo cogente non è stato da subito regolamentato in modo

[229] Un approfondimento sul tema è consultabile in: M. VIOLA DE AZEVEDO ET AL., *La re-identificazione dei dati anonimi e il trattamento dei dati personali per ulteriore finalità: sfide alla privacy*, Ciberspazio e diritto 2010, vol. 11, n. 4, pp. 641-655; altrettanto significativo per quanto concerne l'analisi delle problematiche inerenti il trattamento e la protezione dei dati sanitari conservati nel FSE: S. HAAS, S. WOHLGEMUTH, I. ECHIZEN, N. SONEHARA, G. MÜLLER, *Aspect of privacy for electronic health records*, International Journal of Medical Informatics, 80 (2011) e26-e31.
[230] Tra gli altri, vedasi: D. D'AGOSTINI, A. PIVA, A. RAMPAZZO, *La sicurezza delle informazioni in ambito sanitario*, in "Mondo Digitale", n. 2, 2010, pp. 59-66.

sistematico. Sono, infatti, piuttosto recenti gli interventi legislativi nazionali di cui, un primo concreto esempio è il disegno di legge "Sperimentazione clinica e altre disposizioni in materia sanitaria", approvato dal Consiglio dei Ministri il 24 settembre 2010. Successivi atti normativi di rango primario, di cui si darà conto nel presente capitolo, sono stati perfezionati soltanto a partire dalla fine del 2012.

L'importanza dell'azione intrapresa dagli organi legislativi italiani è evidente: la certezza giuridica che i nuovi istituti acquistano rispetto a quanto in precedenza delineato in via convenzionale.

Scopo della presente rassegna è, anzitutto, mostrare lo stato dell'arte italiano in tema di trattamento dei dati sanitari attraverso l'esame della disciplina vigente; a tal fine, sono stati considerati selezionati provvedimenti particolarmente rilevanti per il dominio in esame, sinteticamente indicati in *figura 11*.

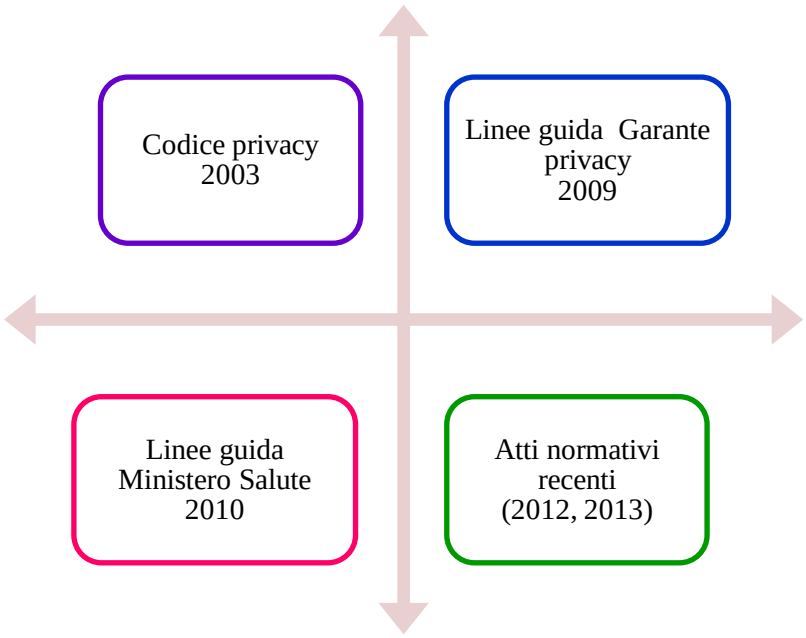


Figura 11 - *Framework* italiano in tema di tutela dei dati sanitari e FSE

5.1 LA DISCIPLINA DEI DATI SANITARI NEL "CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI"

Dando attuazione alla direttiva 95/46/CE[231], il legislatore nazionale si occupa, per la prima volta, di "dati personali idonei a rivelare lo stato di salute di un individuo" nel 1996, e, precisamente, con la legge n. 675[232]; è, comunque, con l'approvazione del "Codice in materia di protezione dei dati personali" (c.d. "Codice *privacy*")[233] che la materia del trattamento di dati personali viene riordinata nel sistema giuridico italiano ed è, quindi, in tale *corpus* che i dati sensibili, di cui quelli sanitari sono una tipologia, trovano la loro disciplina (*cfr. fig. 12*).

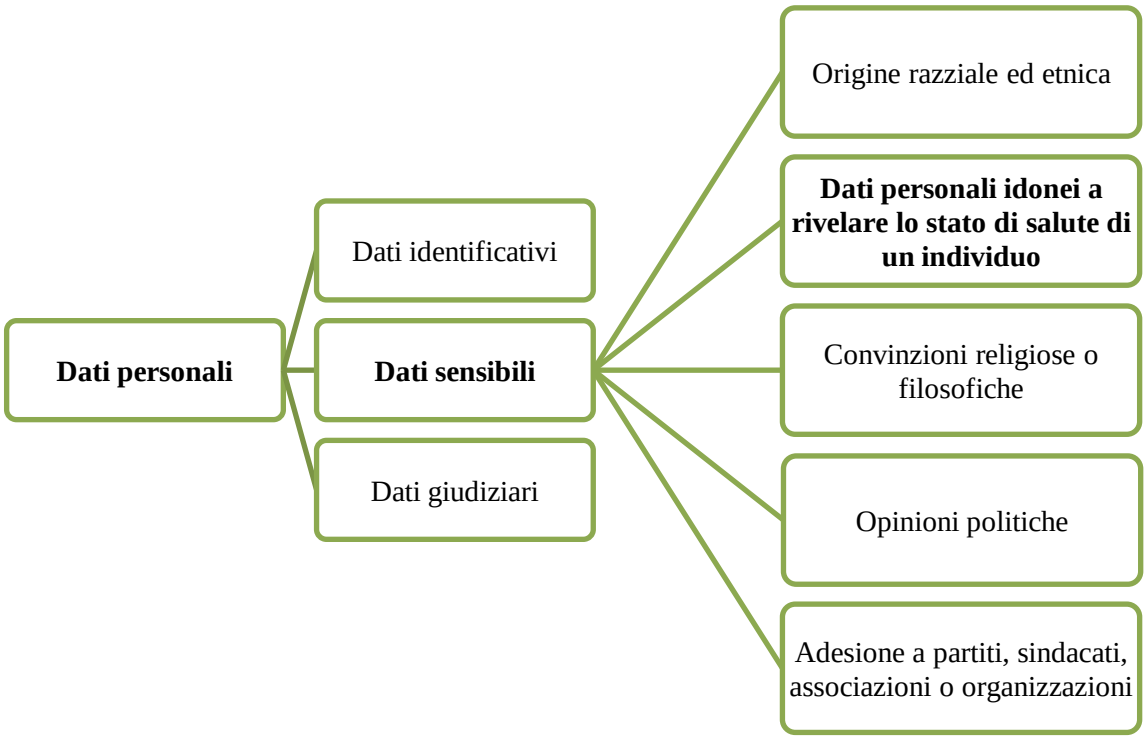


Figura 12 - Tipologia dei dati personali nella legislazione italiana vigente

[231] Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati, pubblicata in G.U. n. L 281 del 23.11.1995.

[232] Legge 31 dicembre 1996 n. 675, *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*, pubblicata in Gazzetta Ufficiale n. 5 del 8.1.1997.

[233] Decreto legislativo 30 giugno 2003 n. 196, *Codice in materia di protezione dei dati personali*, pubblicato in Gazzetta Ufficiale n. 174 del 29.07.2003. Il suddetto decreto è stato predisposto in esecuzione dell'articolo 1 della legge 127/2001, con il quale il Governo riceveva una delega per l'emanazione di un Testo Unico in materia di trattamento dei dati personali e disposizioni connesse; a far data dal 1996, infatti, su delega conferita dalla legge 676/1996 (e successive proroghe - l. 344/1998 e l. 127/2001 -), il Governo aveva emanato ben 10 decreti legislativi aventi ad oggetto il tema della *privacy* (trattasi dei: d.lgs. 123/1997, d.lgs. 255/1997, d.lgs. 135/1998, d.lgs. 171/1998, d.lgs. 389/1998, d.lgs. 51/1999, d.lgs. 135/1999, d.lgs. 281/1999, d.lgs. 282/1999, d.lgs.467/2001).

Il testo normativo in esame, però, analogamente alla direttiva comunitaria, non è dedicato in modo esclusivo alle informazioni sanitarie; per tale ragione, è, quindi, imprescindibile per l'interprete ripercorrere l'intero decreto legislativo 196/2003, al fine di reperire principi e criteri applicabili anche al settore socio-assistenziale.

Come più volte in precedenza segnalato, l'assenza di norme *ad hoc* può generare un vero e proprio disordine non soltanto interpretativo ma anche, e, soprattutto, applicativo, con il rischio di ledere, tra gli altri, il principio di uguaglianza affermato, ad esempio, dall'articolo 3 della Costituzione italiana[234]. Alla luce delle importanti novità introdotte dall'utilizzo crescente di dati e documenti sanitari in formato digitale, appare, pertanto, auspicabile che il legislatore e l'interprete codifichino con certezza la disciplina giuridica, al fine di superare le criticità esistenti.

In apertura, e precisamente all'articolo 1, il "Codice *privacy*" riconosce l'universalità del diritto alla protezione dei dati personali, ribadendo, pertanto, un importante concetto, già sostenuto a livello comunitario, secondo cui la protezione e la libera circolazione dei dati personali del cittadino rappresentano un diritto fondamentale e, al tempo stesso, un bene comune.

Dal punto di vista strutturale, il decreto legislativo è articolato in parti, titoli, capi, sezioni e allegati; aprono la parte I, "disposizioni generali" (artt. 1-45), i primi due titoli, che il legislatore ha riservato a "principi generali" (artt. 1-6) e "diritti dell'interessato" (artt. 7-10). Il titolo III, rubricato "regole generali per il trattamento dei dati", è articolato in tre capi, rispettivamente dedicati a: "[per] tutti i trattamenti" (artt. 11-17), "soggetti pubblici" (artt. 18-22), "privati ed enti pubblici economici" (artt. 23-27).

Oltre all'obbligo di "informativa" di cui all'articolo 13[235], significativo in questa sede richiamare quanto prescritto all'articolo 17 in materia di "trattamento che presenta rischi specifici": i dati c.d. sensibili, proprio per la loro forte connessione con i diritti e le libertà fondamentali e con la dignità dell'individuo, richiedono misure ed accorgimenti a garanzia dell'interessato, misure in dettaglio declinate nel decreto legislativo 196 e di cui saranno fatti cenni nel corso del presente paragrafo.

Ai fini di questo studio, particolarmente interessante è, inoltre, l'articolo 20, rubricato "principi applicabili al trattamento di dati sensibili", ai sensi del quale è necessario che, per

[234] La norma invocata così recita: "1. Tutti i cittadini hanno pari dignità sociale e sono eguali davanti alla legge, senza distinzione di sesso, di razza, di lingua, di religione, di opinioni politiche, di condizioni personali e sociali. 2. È compito della Repubblica rimuovere gli ostacoli di ordine economico e sociale, che, limitando di fatto la libertà e l'eguaglianza dei cittadini, impediscono il pieno sviluppo della persona umana e l'effettiva partecipazione di tutti i lavoratori all'organizzazione politica, economica e sociale del Paese".
[235] *Cfr*. Appendice.

i soggetti pubblici, siano predisposte specifiche previsioni normative che regolino tipologia di dati trattabili, operazioni eseguibili nonché finalità di interesse pubblico perseguite con l'attività di trattamento.

Così come previsto dal secondo comma della norma in esame, laddove tali disposizioni siano incomplete o addirittura assenti, "il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g), anche su schemi tipo. Qualora il trattamento non sia previsto da alcuna disposizione di legge - prosegue il terzo comma - i soggetti pubblici possono richiedere al Garante l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi dell'articolo 26, comma 2, il trattamento dei dati sensibili. Il trattamento è consentito solo se il soggetto pubblico provvede altresì a identificare e rendere pubblici i tipi di dati e di operazioni nei modi di cui al comma 2".

Il titolo IV del decreto legislativo 196/2003 raccoglie, invece, le disposizioni riguardanti i "soggetti che effettuano il trattamento" (artt. 28-30), quali titolare, responsabile e incaricato[236]; il titolo V, "sicurezza dei dati e dei sistemi", contiene al capo I le norme in materia di "misure di sicurezza" (artt. 31-32-*bis*) ed al capo II quelle dedicate alle "misure minime di sicurezza" (artt. 33-36)[237].

In particolare, l'articolo 34, rubricato "trattamenti con strumenti elettronici", nel ribadire che il trattamento di dati personali con strumenti digitali è possibile solo nei modi e limiti di cui al "Disciplinare tecnico in materia di misure minime di sicurezza" (contenuto

[236] Tra gli altri: A. FLORIO, *Il trattamento dei "dati idonei a rivelare lo stato di salute" da parte dei medici liberi professionisti*, in Ciberspazio e Diritto, 2010, vol. 11, n. 1, pp. 111-145; C. DI COCCO, *Soggetti che effettuano il trattamento (Parte I-Titolo IV)*, in J. MONDUCCI, G. SARTOR, *Il codice in materia di protezione dei dati personali*, CEDAM, Padova, 2004, pp. 119-156.

[237] Per approfondimenti, si rinvia a: P. PERRI, *Privacy, diritto e sicurezza informatica*, Giuffrè, Milano, 2007, pp. 195 ss.; C. RABAZZI, P. PERRI, G. ZICCARDI, *La sicurezza informatica e la Privacy*, in G. ZICCARDI (a cura di), *Telematica giuridica. Utilizzo avanzato delle nuove tecnologie da parte del professionista del diritto*, Giuffrè, Milano, 2005, pp. 516 e ss.; P. PERRI, *Le misure di sicurezza*, in J. MONDUCCI, G. SARTOR, *Il codice in materia di protezione dei dati personali*, CEDAM, Padova, 2004, pp. 137 e ss.; G. CORASANITI, *La sicurezza dei dati personali*, in CARDARELLI, SICA, ZENO-ZENCOVICH (a cura di), *Il codice dei dati personali. Temi e problemi*, Giuffrè, Milano, 2004, pp. 112-163; P. PERRI, *Introduzione alla sicurezza informatica e giuridica*, in E. PATTARO (a cura di), *Manuale di diritto dell'informatica e delle nuove tecnologie*, Clueb s.c.a.r.l., Bologna, 2002, pp. 306 e ss.

nell'allegato B) del "Codice *privacy*"[238]), sancisce, al primo comma, l'obbligatorietà dell'utilizzo di misure minime di sicurezza (già peraltro ricordate nei paragrafi della presente ricerca ad esse dedicati), quali: "a) autenticazione informatica; b) adozione di procedure di gestione delle credenziali di autenticazione; c) utilizzazione di un sistema di autorizzazione; d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici; e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici; f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi; g)[239]; h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari".

In chiosa alla parte I si trovano i titoli VI e VII, in cui sono rispettivamente raccolte norme su "adempimenti" (artt. 37-41) e "trasferimento dei dati all'estero" (artt. 42-45).

La parte II del "Codice *privacy*" prevede "disposizioni relative a specifici settori" (artt. 46-140); per ciò che concerne la presente ricerca, significativo è il titolo V, dedicato al "trattamento di dati personali in ambito sanitario" (artt. 75-94), nel quale sono regolate le modalità di trattamento delle informazioni idonee a rivelare lo stato di salute per esercenti le professioni sanitarie ed organismi sanitari pubblici.

Una prima puntualizzazione è a questo punto necessaria: nella definizione normativa di cui al d.lgs. 196/2003, il "dato sanitario" si qualifica come tale - e, quindi si distingue dal "dato sensibile", richiedendo una disciplina *ad hoc* (*cfr. fig. 12*) - per le seguenti caratteristiche: a) occorre, anzitutto, che sia riferito ad una persona identificata o identificabile (non sia, dunque, anonimo); b) è necessario che venga trattato da un soggetto esercente la professione sanitaria o comunque da un organismo sanitario; c) è indispensabile che sia raccolto per finalità di trattamento esclusive, quali la tutela della salute del paziente, di un terzo o della collettività. Per contro, laddove vengano meno

[238] L'allegato B), "Disciplinare tecnico in materia di misure minime di sicurezza", in riferimento agli articoli 33-36 del Codice, indica le "modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici"; sono, in particolare, declinati il "sistema di autenticazione informatica", il "sistema di autorizzazione", misure di aggiornamento periodico, "misure in caso di trattamento di dati sensibili o giudiziari", "misure di tutela e garanzia". In chiosa al disciplinare sono, altresì, previste le "modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici".

[239] La lettera g) è stata soppressa dal d.l. 9 febbraio 2012, n. 5, convertito con modificazioni dalla l. 4 aprile 2012, n. 35.

questi requisiti, la disciplina giuridica che si applicherà ai dati raccolti sarà quella generale, relativa ai dati sensibili.

Una seconda precisazione riguarda, poi, la natura stessa del "dato sanitario": secondo quanto disposto dalla normativa in esame, esso si riferisce non soltanto all'informazione che "rivela" lo stato di salute del'interessato (aspetto questo già previsto dalla direttiva 95/46/CE), ma anche all'informazione "idonea a rivelare" lo stato di salute dell'interessato.

Per quanto riguarda le ipotesi di trattamento considerate dal legislatore, esse possono essere così sintetizzate: i) trattamento con il consenso dell'interessato ed anche senza l'autorizzazione del Garante, nel caso di dati ed operazioni indispensabili per perseguire una finalità di tutela della salute o dell'incolumità fisica dell'interessato; ii) trattamento anche senza il consenso dell'interessato, previa autorizzazione rilasciata del Garante, sentito il Consiglio Superiore di Sanità, se tale finalità riguarda un terzo o la collettività[240].

Alle due circostanze indicate, va aggiunta un'altra fattispecie, rappresentata dalle emergenze sanitarie, per le quali l'informativa ed il consenso al trattamento dei dati personali possono intervenire successivamente alla prestazione; la medesima previsione è stabilita nelle ipotesi in cui l'attività medica possa essere pregiudicata dall'acquisizione preventiva del consenso, in termini di tempestività o efficacia e, in particolare, nei casi di tutela urgente della salute, tra cui rientrano: a) impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, quando non è possibile acquisire il consenso da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato; b) rischio grave, imminente e irreparabile per la salute o l'incolumità fisica dell'interessato.

Proseguendo nella lettura del titolo V del "Codice *privacy*", altrettanto rilevante è la previsione di cui all'articolo 92, rubricato "cartelle cliniche", da cui emerge il valore giuridico di atto amministrativo che questi preziosi documenti sanitari rivestono. Da tale *status* deriva non soltanto la validità giuridica dei documenti informatici in esame ma anche, e soprattutto, l'efficacia probatoria degli stessi. Interessante in proposito notare come nell'epoca della dematerializzazione la *ratio iuris* applicata all'efficacia probatoria dei documenti analogici sia rimasta immutata, e ciò, anche grazie all'introduzione di strumenti tecnologici, quali ad esempio la firma elettronica avanzata, idonei a garantire la

[240] In questi casi il consenso può essere prestato con modalità semplificate: anziché con atto scritto dell'interessato, con un'unica dichiarazione, anche orale, annotata dall'esercente la professione sanitaria o dall'organismo sanitario pubblico.

paternità degli atti. Quanto osservato, è per analogia applicabile al dato sanitario digitale raccolto nel Fascicolo Sanitario Elettronico, sebbene si debba dar conto che la dottrina non è del tutto concorde su tale conclusione e richieda un intervento chiarificatore da parte del legislatore[241].

Ritornando al contenuto della norma, il "Codice in materia di protezione dei dati personali" prevede che, per la redazione e la conservazione delle cartelle cliniche, è indispensabile che gli organismi sanitari pubblici e privati assicurino la comprensibilità dei dati, di cui, la distinzione tra le informazioni relative al paziente e quelle eventualmente riguardanti altri interessati è un aspetto centrale. Per far valere o difendere un diritto dell'assistito ovvero per tutelare una situazione giuridicamente rilevante, sono, altresì, ammissibili la presa visione o il rilascio di copia della cartella e dell'acclusa scheda di dimissione ospedaliera, da parte di soggetti diversi dall'interessato.

Chiude il titolo V della parte II del d.lgs. 196/2003 l'articolo 94, ai sensi del quale è ammissibile il trattamento di dati idonei a rivelare lo stato di salute contenuti in banche di dati, schedari, archivi o registri tenuti in ambito sanitario, purché effettuato nel rispetto del "principio di necessità nel trattamento dei dati" sancito dall'articolo 3 dello stesso decreto, secondo cui, occorre ridurre al minimo il trattamento di dati identificativi (anche da parte di sistemi informativi e programmi informatici), prediligendo piuttosto, ove possibile, l'utilizzo di dati anonimi e de-identificati.

Si noti, a riguardo, l'assenza di tipizzazione delle misure cui il legislatore idealmente rinvia, rimettendo ai gestori delle banche dati la scelta degli strumenti tecnologici adeguati allo scopo.

5.2 LE "LINEE GUIDA IN TEMA DI FASCICOLO SANITARIO ELETTRONICO E DI *DOSSIER* SANITARIO" DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In assenza di norme cogenti di carattere primario o secondario, scopo delle "Linee guida in tema di fascicolo sanitario elettronico e di *dossier* sanitario" del Garante per la protezione dei dati personali[242], redatte nel 2009, fu la previsione di precipue ed adeguate garanzie per il beneficiario principale dei servizi di *e-Health*, il cittadino/utente.

---

[241] Questo concetto è stato ripreso ed approfondito in MINISTERO DELLA SALUTE, *Il Fascicolo Sanitario Elettronico. Linee guida nazionali*, Roma, 11 novembre 2010, pp. 28, a cui è dedicato il paragrafo seguente della presente ricerca.

[242] Le "Linee guida" del 16 luglio 2009 sono, tra l'altro, conseguenza dei lavori preparatori raccolti in ARTICLE 29 DATA PROTECTION WORKING PARTY, *Working Document on the processing of personal data relating to health in electronic health records (EHR) - Adopted on 15 February 2007*, 00323/07/EN, WP

Come si evince dallo stesso titolo, i dati sanitari oggetto delle "Linee guida" sono sia quelli salvati nel "*dossier* sanitario", ivi definito come "strumento costituito presso un organismo sanitario in qualità di unico titolare del trattamento al cui interno operino più professionisti", sia quelli raccolti nel Fascicolo Sanitario Elettronico, ovvero "il fascicolo formato con riferimento a dati sanitari originati da diversi titolari del trattamento operanti più frequentemente, ma non esclusivamente, in un medesimo ambito territoriale".

Il documento in esame, così come dichiarato dalla stessa Autorità garante, se, da una parte, tiene conto delle importanti iniziative di gestione informatica e telematica di atti, documenti e procedure finalizzate alla dematerializzazione dell'apparato sanitario italiano, dall'altra mostra speciale interesse per il crescente fenomeno dell'interoperabilità dei sistemi informativi (a cui sono stati, peraltro, dedicati approfondimenti di carattere legislativo e tecnico nei capitoli precedenti), interoperabilità che, al tempo stesso, crea maggiori rischi per i dati personali dei pazienti e, richiede, pertanto, la predisposizione di adeguati meccanismi per garantire la tutela della *privacy* e della riservatezza. Sistemi complessi, infatti, talora appartenenti a giurisdizioni diverse, espongono i singoli ad una vulnerabilità più ampia rispetto a quella esistente nei casi di produzione cartacea delle "cartelle clinico-sanitarie"; tecniche di anonimizzazione, de-identificazione, separazione degli accessi ai dati, sono, in questo senso, basilari, soprattutto nei casi in cui, alle finalità di prevenzione, diagnosi, cura e riabilitazione dell'interessato, siano associati utilizzi delle informazioni personali per motivi amministrativi o fini di ricerca scientifica, epidemiologica o statistica.

Analogamente a quanto accade per i profili tecnici, anche per quanto concerne quelli giuridici, si può notare che la questione dell'interoperabilità è egualmente rilevante, soprattutto in un contesto storico, come quello attuale, fortemente contrassegnato dalla mobilità transfrontaliera[243]. In proposito si tenga conto dei problemi derivanti dalla pluralità di giurisdizioni e, conseguentemente di istituti giuridici, esistenti a livello

131, in cui sono forniti orientamenti sull'interpretazione del quadro giuridico in materia di *privacy* applicabile al Fascicolo Sanitario Elettronico nonché indicazioni su requisiti e garanzie necessari per la protezione dei dati ai nuovi strumenti di sanità digitale. Tra essi: "*1. Respecting self determination; 2. Identification and authentication of patients and health care professionals; 3. Authorization for accessing EHR in order to read and write in EHR; 4. Use of EHR for other purposes; 5. Organisational structure of an EHR system; 6. Categories of data stored in EHR and modes of their presentation; 7. International transfer of medical records; 8. Data security; 9. Transparency; 10. Liability issues; 11. Control mechanisms for processing data in EHR*".

[243] Interessante in proposito ricordare che, al fine di rafforzare la continuità delle cure e garantire l'accesso ad un'assistenza sanitaria sicura, con la direttiva 2011/24/UE è stata istituita "*eHealth Network*", una rete volontaria tra le autorità nazionali responsabili dell'assistenza sanitaria *online*, per la prima volta riunitasi in occasione della "*eHealth Conference 2012*".

nazionale; a titolo esemplificativo, le garanzie sulla base delle quali è stato rilasciato un consenso al trattamento dei dati in un Paese "A", verosimilmente potrebbero non corrispondere a quelle esistenti in un Paese "B". *Quid iuris* dunque?

Esaminati i profili generali della sanità elettronica e definito l'ambito di applicazione delle "Linee guida", l'Autorità garante dedica la parte II alle "garanzie per l'interessato", di cui il "diritto alla costituzione di un Fascicolo Sanitario Elettronico" (e cioè il diritto alla collezione di dati ed informazioni inerenti la storia sanitaria del singolo assistito) rappresenta un diritto essenziale.

Tuttavia, la possibilità per il cittadino/paziente di avvalersi o meno di questo strumento di *e-Health*, e, quindi la sua non obbligatorietà, è, anzitutto, conseguenza del fatto che, nel 2009, anno di redazione delle "Linee guida", nell'ordinamento giuridico italiano non esistevano norme imperative, di carattere primario o secondario, che imponessero agli enti del Sistema Sanitario Nazionale di adottarlo, e ciò, sebbene ne fossero già riconosciuti, sia per i sistemi stessi, sia per gli utenti, i vantaggi illustrati nei capitoli precedenti.

Conformemente a quanto previsto in tema di trattamento dei dati personali (e precisamente agli articoli 75 e seguenti del "Codice *privacy*"), anche nelle "Linee guida" il Garante ha introdotto il c.d. principio di autodeterminazione, secondo cui l'utente ha la libera facoltà di autorizzare alla costituzione di un fascicolo elettronico nonché decidere se, e per quali dati, rilasciare il consenso al trattamento, consenso che, peraltro, oltre ad essere informato, deve sempre essere autonomo e specifico. Il FSE non è, infatti, un "*unicum*" immutabile, bensì una raccolta di dati e documenti sanitari che, in quanto tali, sono tra loro distinti.

In termini di responsabilità professionale, rilevante è evidenziare la distanza abissale tra ciò che accade nel caso della cartella clinico-sanitaria fruibile in formato digitale e del Fascicolo Sanitario Elettronico (così come descritto nelle "Linee guida" del 2009): in questa seconda ipotesi, infatti, il medico è soltanto uno dei soggetti che, insieme al consumatore, gestisce la raccolta di dati; per tale ragione, non è responsabile "*a priori*" dei contenuti del fascicolo, il quale, a sua volta, non dovrà necessariamente rispettare i requisiti di completezza ed accuratezza prescritti per la cartella clinica[244].

Altro diritto riconosciuto all'assistito è l'oscuramento dei dati: il titolare del trattamento deve cioè garantire che talune informazioni concernenti lo stato di salute dell'interessato

[244] Il valore legale delle diverse fattispecie di dati e documenti presenti nel FSE è regolato dall'articolo 2702 codice civile nonché dalle regole tecniche (requisiti di firme elettronica qualificata/firma digitale e di marcatura temporale) di cui al DPCM 30 marzo 2009 recante appunto "Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici".

possano non essere visibili dai soggetti autorizzati alla consultazione del FSE[245]; altra circostanza ammessa è il c.d. oscuramento dell'oscuramento, inteso come l'ulteriore diritto, riconosciuto a chi ha esercitato l'oscuramento dei dati, di far sì che non sia visibile, a quanti sono autorizzati all'accesso al fascicolo sanitario, quali informazioni il paziente ha deciso di non divulgare/oscurare.

L'incompletezza della storia clinica che ne consegue dev'essere segnalata come probabile dal titolare del trattamento ai soggetti autorizzati ad accedere al Fascicolo Sanitario Elettronico. Da ciò si evince la dicotomia tra il principio di autodeterminazione e quello di completezza ed accuratezza previsto, invece, per la redazione della cartella sanitaria, principio da cui, come già osservato, deriva la responsabilità professionale del sanitario.

Ulteriore aspetto considerato dal Garante concerne il possibile inserimento di informazioni di salute (pregresse alla costituzione del FSE) o l'eventuale revoca di taluni dati inseriti nel FSE (con la conseguente non implementazione della cartella digitale): in entrambe le circostanze, il titolare del trattamento deve garantire al paziente le summenzionate facoltà, ed in particolare, nel primo caso, solo previo rilascio di un consenso specifico ed informato.

Le finalità di prevenzione, diagnosi e cura dell'interessato, uniche finalità per le quali è ammessa la raccolta ed il trattamento dei dati sanitari[246], hanno indotto il Garante a ribadire che unici titolari del trattamento dei dati debbano essere gli esercenti le professioni sanitarie, con esclusione di periti, compagnie di assicurazione, datori di lavoro, associazioni o organizzazioni scientifiche e organismi amministrativi anche operanti in ambito sanitario, nonché il personale medico nell'esercizio di attività medico-legale[247].

---

[245] Come ricordato dal Garante per la protezione dei dati personali nelle "Linee guida" in esame, tra le informazioni "oscurate per legge", in quanto oggetto di specifiche disposizioni normative, rientrano quelle a tutela delle vittime di atti di violenza sessuale o di pedofilia (l. 66/1996, l. 269/1998, l. 38/2006), delle persone sieropositive (l. 135/1990), di chi fa uso di sostanze stupefacenti, di sostanze psicotrope e di alcool (D.P.R. 309/1990), delle donne che si sottopongono a un intervento di interruzione volontaria della gravidanza o che decidono di partorire in anonimato (l. 194/1978, d.m. 349/2001), nonché con riferimento ai servizi offerti dai consultori familiari (l. 405/1975).

[246] Come si dirà più avanti, l'esclusività di trattamento per finalità di prevenzione, diagnosi e cura è stata rivista con l'introduzione dei più recenti provvedimenti legislativi, nei quali è ammesso, seppur in modo condizionato all'adozione di precipue misure di sicurezza, il trattamento dei dati per finalità di studio e ricerca, programmazione sanitaria etc.

[247] In proposito, commenta Moruzzi, la disciplina per il trattamento dei dati da parte degli "esercenti le professioni sanitarie" e degli organismi sanitari pubblici, è parzialmente derogatoria rispetto a quella prevista per il trattamento dei medesimi dati da parte dei soggetti pubblici, giacché tali soggetti, anche senza l'autorizzazione del Garante, possono trattare i dati, limitatamente alle operazioni indispensabili per il perseguimento della tutela dell'incolumità fisica e della salute dell'interessato, previo consenso del medesimo. L'Autore considera, inoltre, che: "le finalità che possono essere perseguite attraverso il FSE ed il dossier sanitario - in assenza di una normativa specifica che autorizzi espressamente altre forme di

Un profilo centrale segnalato dal Garante investe, inoltre, le esigenze di formazione inerenti le modalità di creazione ed utilizzazione dei fascicoli sanitari elettronici per i soggetti legittimati alla loro consultazione.

Questo tassello, introdotto nelle "Linee guida", rinvia all'urgenza di una capillare alfabetizzazione sull'uso delle nuove tecnologie, e, più in generale, sulla divulgazione di conoscenze e competenze in materia di Tecnologie dell'Informazione e delle Comunicazioni. I livelli di *digital divide* presenti sul territorio nazionale sono, infatti, a tutt'oggi elevati e, purtroppo, frequentemente investono tutte le fasce della popolazione, non soltanto quelle più svantaggiate, seppur in modo diversificato a seconda delle zone territoriali del Paese[248]. Non di secondaria rilevanza, la mancata distribuzione uniforme sul territorio nazionale di banda larga, concausa del divario digitale.

Le indicazioni del Garante considerano, altresì, il tema dell'accesso ai dati personali raccolti nei fascicoli sanitari elettronici; in questa ipotesi sono da osservare le previsioni di cui all'articolo 7 del "Codice *privacy*", rubricato "diritto di accesso ai dati personali ed altri diritti"[249].

Per favorire il paziente nell'esprime scelte consapevoli, è necessario che il titolare del trattamento fornisca un'informativa chiara, specifica, *ad hoc*, così come, specifico e *ad hoc*, è il consenso richiesto al consumatore in merito al trattamento dei dati personali sanitari; l'ipotesi di un eventuale diniego da parte del paziente alla costituzione di un FSE non inficia, in alcun modo, il diritto di fruire delle cure necessarie, e ciò, soprattutto, considerati, da una parte il rango costituzionale del diritto alla salute riconosciuto dall'articolo 32, dall'altra l'organizzazione assistenziale del Sistema Sanitario Nazionale che ne deriva.

---

utilizzazione - vanno ricondotte alla cura, con esclusione di ogni alta finalità, in particolare finalità amministrative proprie delle Regioni o dello Stato, ferme restando eventuali esigenze in ambito penale. Sono viceversa ammesse quelle finalità amministrative strettamente connesse all'erogazione della prestazione sanitaria, nel qual caso però il FSE e il dossier sanitario dovranno essere strutturati in modo che i dati amministrativi siano separati dalle informazioni sanitarie. L'eventuale utilizzo del FSE e del dossier anche per fini di ricerca scientifica, epidemiologica o statistica non è di per sé precluso, ma, precisa il Garante, «può avvenire solo in conformità alla normativa di settore ed essere oggetto di preventiva e specifica attenzione, anche nei casi in cui la tenuta dell'elenco degli eventi sanitari riguardante un determinato interessato sia demandata ad un'infrastruttura regionale. Deve invece ritenersi precluso il trattamento di dati personali attraverso il FSE/dossier, da parte dei periti, compagnie di assicurazione, datori di lavoro, associazioni o organizzazioni scientifiche, organismi amministrativi anche operanti in ambito sanitario, nonché del personale medico nell'esercizio di attività medico-legale. A tali soggetti deve essere precluso l'accesso al FSE/dossier costituito per finalità esclusive di salute»" in M. MORUZZI, *e–Health e Fascicolo Sanitario Elettronico*, Il Sole 24 ore, Milano, 2009, pp. 155-156 e 160-161.

[248] Di questo tema sono già stati forniti dei cenni nel capitolo primo della presente ricerca.

[249] *Cfr*. Appendice.

La natura stessa dei dati "sensibili" sulla salute, per le ragioni che più volte sono state sottolineate nella presente ricerca, necessita di idonei livelli di sicurezza, volti a prevenire accessi abusivi ai dati nonché furti o smarrimenti di supporti di memorizzazione e sistemi di elaborazione. Tale evidenza, insieme alla consapevolezza di un impegno ulteriore da parte degli enti sanitari in questo settore, hanno indotto il Garante per la protezione dei dati personali a soffermarsi nuovamente sulle "misure di sicurezza".

Inevitabile, in proposito, il richiamo alle norme del "Codice *privacy*" (in particolare, agli articoli 31 e ss.), nonché l'indicazione precisa delle seguenti misure: "sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli e delle esigenze di accesso e trattamento; procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli incaricati; individuazione di criteri per la cifratura o per la separazione dei dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali; tracciabilità degli accessi e delle operazioni effettuate; sistemi di *audit log* per il controllo degli accessi al *database* e per il rilevamento di eventuali anomalie", cui, si aggiungono "protocolli di comunicazione sicuri basati sull'utilizzo di *standard* crittografici per la comunicazione elettronica dei dati tra i diversi titolari coinvolti".

Un problema lasciato aperto dalle "Linee guida in tema di fascicolo sanitario elettronico e di *dossier* sanitario" del Garante per la protezione dei dati personali è quello relativo all'architettura giuridica del FSE, termine con cui qui si rinvia alla questione della titolarità nonché responsabilità del trattamento dei dati sanitari oggetto di questo strumento digitale.

L'assenza di un intervento specifico da parte del Garante nelle "Linee guida" costringe l'interprete a richiamare quanto in proposito disposto dal decreto legislativo 196/2003; entrambe le figure, di "titolare" e "responsabile" del trattamento, sono definite dall'articolo 4, rispettivamente alle lettere (f) e (g): è "titolare" del trattamento "la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza"; è, invece, "responsabile" del trattamento dei dati "la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali".

É a tutt'oggi controverso delineare quale modello di responsabilità sarebbe preferibile adottare in riferimento al contesto sanitario: i) se quello della contitolarità, nel quale l'azione compiuta dal titolare dei dati è unica (in quanto il titolare agisce da solo, ad

esempio nella sua funzione di azienda ospedaliera o di azienda sanitaria locale); ii) se quello della titolarità congiunta, modello che implica la cogestione dei dati in ogni fase del trattamento, dal momento del rilascio del consenso fino alla fine (in questo caso l'azienda ospedaliera o la ASL dovrebbero operare in modo costante congiuntamente alle aziende regionali); iii) se, infine, un modello di corresponsabilità tra il titolare ed i soggetti da lui designati. Lo stato dell'arte italiano dimostra che il modello oggi scelto è quello della con titolarità, che predilige una titolarità autonoma, in un certo senso rispettosa della natura stessa del FSE, strumento volto a collezionare i dati concernenti la storia del paziente. Sebbene tale architettura appaia la migliore rispetto a quella degli altri modelli ricordati, tuttavia, non si può non riconoscere che una sua corretta attuazione richiede un notevole sforzo di coordinamento tra tutti i soggetti coinvolti. In questo scenario, non secondario, inoltre, il ruolo svolto dalle Regioni, vero e proprio motore sia in termini di coordinamento sia, talora, in termini di finanziamento, di molti progetti in essere a livello nazionale per la realizzazione ed implementazione del FSE. Nonostante le importanti funzioni esercitate, il ruolo ricoperto dalle Regioni non è in alcun modo previsto dal "Codice *privacy*", nel quale, il concetto di trattamento (e conseguentemente di titolare del trattamento) afferisce esclusivamente alle operazioni "sui" dati. In altre parole, il mero coinvolgimento nell'attività propulsiva di sviluppo del contesto di *e-Health* è di per sé insufficiente, ai sensi della normativa vigente, ai fini della responsabilità giuridica.

5.3 "IL FASCICOLO SANITARIO ELETTRONICO. LINEE GUIDA NAZIONALI" DEL MINISTRO DELLA SALUTE

Come ricordato nel "Capitolo Secondo" e, precisamente al paragrafo 3.4, le "Linee guida nazionali" in materia di Fascicolo Sanitario Elettronico sono state presentate nel 2010 dal Ministero della Salute, a conclusione dei lavori di un Tavolo interistituzionale istituito nel 2008 dal Ministero della Salute e da esso coordinato, al quale parteciparono esperti del Ministero, rappresentanti delle Regioni designati dalla Commissione salute, del Dipartimento per la digitalizzazione della pubblica amministrazione e l'innovazione tecnologica della Presidenza del Consiglio dei Ministri, dell'ente per la digitalizzazione della Pubblica amministrazione "DigitPa" e dell'Autorità Garante per il trattamento dei dati personali[250].

[250] *Cfr*. MINISTERO DELLA SALUTE, *Il Fascicolo Sanitario Elettronico. Linee guida nazionali*, Roma, 11 novembre 2010, pp. 28.

Scopo principale di questo documento programmatico fu indicare gli elementi necessari alla realizzazione nazionale omogenea di un Fascicolo Sanitario Elettronico, e ciò, soprattutto, considerati i molti progetti regionali esistenti, nei quali spesso, tuttavia, sono stati adottati modelli architetturali, *standard* semantici, infrastrutture, che, per la loro eterogeneità, mal si confanno all'idea di interoperabilità auspicata dalla Commissione europea.

Obiettivo finale del documento fu, pertanto, creare un sostrato comune tra le regioni italiane per la realizzazione ed implementazione di un sistema informativo sanitario nazionale condiviso, attraverso l'individuazione di principi di diritto e profili tecnici condivisi; analogamente a quanto osservato in precedenza, trattasi, però, di "Linee guida nazionali" che, sebbene provengano dall'ente sanitario gerarchicamente competente a definire il quadro giuridico, operativo e finanziario in materia di salute, non acquisiscono, però, rango normativo primario.

Oggetto delle "Linee guida" è, dunque, il Fascicolo Sanitario Elettronico. Nel proporre una definizione di questo strumento digitale, il Ministero della Salute sottolinea aspetti diversi rispetto a quanto proposto dal Garante per la protezione dei dati personali nelle "Linee guida in tema di Fascicolo sanitario elettronico e di *dossier* sanitario", in cui l'accento verteva sulla figura del "titolare del trattamento dei dati": ciò che, infatti, secondo l'Autorità garante differenzia il "FSE" dal "*dossier* sanitario" è proprio il fatto che le informazioni raccolte nel FSE sono originate da diversi titolari.

Nel caso delle "Linee guida nazionali", invece, assumono un ruolo centrale la dimensione della storia clinica del paziente, la funzione dell'arte medica e la continuità assistenziale nonché la finalità "di prevenzione, diagnosi, cura e riabilitazione" del FSE. A ciò aggiungasi il *focus* sulla tipologia di dati e documenti che compongono il Fascicolo Sanitario Elettronico: pur essendo in formato digitale, e non più quindi cartaceo, essi non mutano il loro valore legale: cambia, infatti, la forma ma non il contenuto del singolo referto, esame di laboratorio, prescrizione medico-diagnostica etc. La certezza giuridica conferita ai dati sanitari digitali è resa possibile grazie all'adozione di misure tecniche specifiche, previste *ex lege*, di cui sono esempi la firma elettronica qualificata/firma digitale e la marcatura temporale[251].

[251] Secondo quanto evidenziato dallo stesso Ministero della Salute nelle "Linee guida nazionali", "il valore legale (*ex* articolo 2702 del codice civile) delle diverse fattispecie di dati e documenti potenzialmente presenti nel FSE è dunque da rinvenirsi nelle disposizioni della suddetta norma e nelle vigenti regole tecniche di cui al DPCM 30 marzo 2009 recante "Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici", che possono sintetizzarsi

Nel documento del 2010 non mancano, inoltre, i riferimenti all'interoperabilità, alle problematiche connesse al tema della *privacy*, alle numerose relazioni amministrative ed organizzative che si innestano nell'erogazione dei servizi e nella presa in carico dei processi di cura[252].

Per la predisposizione di un modello di "Fascicolo Sanitario Elettronico" e di "*Patient Summary*" nazionali, il Ministero della Salute individua puntuali "contenuti minimi" da inserire in fase di progettazione.

Nel primo caso trattasi di "dati identificativi dell'assistito" (seppur gestiti in archivi separati dal FSE, tali dati rappresentano l'elemento identificativo basilare dell'utente; per tale ragione, correttezza e validità - verificabili attraverso la richiesta al titolare dei dati stessi - sono requisiti essenziali per un efficiente funzionamento del sistema di diagnosi e cura)[253], "dati amministrativi relativi dell'assistenza" (che definiscono, tra l'altro, la posizione del paziente rispetto al Servizio Sanitario Nazionale)[254], "documenti sanitari e socio-sanitari" (non trattandosi di un *unicum*, bensì di una vera e propria raccolta di dati e documenti del paziente, il FSE è una collezione che si alimenta nel tempo e di cui fanno parte documenti minimi, resi disponibili a livello regionale, ed altri aggiornamenti; se conferita l'autorizzazione del paziente, il FSE può addirittura contenere informazioni di salute precedenti alla costituzione del documento digitale)[255].

Nel secondo caso, quello cioè del "*Patient Summary*" - inteso come "Profilo Sanitario Sintetico" del paziente, creato ed aggiornato dal Medico di Medicina Generale o Pediatra di Libera Scelta, destinato a diversi soggetti per finalità di cura - le informazioni minime da

---

nell'adempimento dei requisiti di firma elettronica qualificata/firma digitale e di marcatura temporale" (in ivi, p. 8).

[252] Il Fascicolo Sanitario Elettronico è definito, infatti, come "l'insieme di dati e documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito, che ha come scopo principale quello di agevolare l'assistenza al paziente, offrire un servizio che può facilitare l'integrazione delle diverse competenze professionali, fornire una base informativa consistente, contribuendo al miglioramento di tutte le attività assistenziali e di cura, nel rispetto delle normative per la protezione dei dati personali" (in ivi, p. 7).

[253] Di cui fanno parte: "Cognome (alla nascita), Nome, Sesso, Data di Nascita, Comune di Nascita, Provincia di nascita, Indirizzo di Residenza, Indirizzo di Domicilio, Data di Decesso (data di chiusura del fascicolo)".

[254] Ne sono specifiche l'indicazione di: "ASL Appartenenza, Data Inizio del periodo di assistenza presso la ASL, Data scadenza del periodo di assistenza presso la ASL (valorizzata solo se prevista), Codice Fiscale Medico, Cognome Medico, Nome Medico, Data Inizio periodo di assistenza presso il medico, Data Fine periodo di assistenza presso il medico (valorizzata solo se prevista), Tipo Assistenza (generici/pediatri, altro), Recapiti medico (indirizzo, telefono, etc.), Altro, Esenzioni e relative eventuale scadenza".

[255] Costituisce il "nucleo minimo di documenti" la seguente tipologia di documenti: "Referti, Verbali Pronto Soccorso, Lettere di dimissione, Profilo Sanitario Sintetico". Altri documenti che possono integrare il FSE sono: "Prescrizioni (specialistiche, farmaceutiche, ecc.), Cartelle cliniche di ricovero (ordinario e *day* hospital), Bilanci di Salute, Assistenza Domiciliare: scheda, programma e cartella clinica, Piani terapeutici, Assistenza residenziale e semiresidenziale: scheda multidimensionale di valutazione, Erogazione farmaci, Certificati".

prevedere sono: "intestazione" (nella quale vanno indicati "dati del paziente", "dati del medico", "eventuali nominativi da contattare"), "dati essenziali" (quali "allergie, reazioni avverse ai farmaci o ai mezzi di contrasto o ad altre sostanze, intolleranze, rischi immunitari", "problemi di salute rilevanti e diagnosi", "terapie in corso", "stato del paziente", "trattamenti e procedure terapeutiche, chirurgiche e diagnostiche", "fattori di rischio", "vaccinazioni", "organi mancanti/trapianti/espianti", "protesi, impianti, ausili"), "altre informazioni sul paziente" ("parametri di monitoraggio", "piano di cura attivo", "gruppo sanguigno", "altre patologie di recente insorgenza", "gravidanza e parto", "assenso/dissenso alla donazione d'organi"[256]). Informazioni opzionali possono, infine, riguardare "accertamenti", "visite effettuate dal medico di famiglia", "patologie non croniche".

Preso atto dell'evoluzione degli strumenti di *e-Health* (di cui i *Personal Health Device* sono un significativo emergente prototipo), e del conseguente crescente livello di *empowerment* dei pazienti, il Ministero della Salute ha, inoltre, indicato la possibilità che il FSE contenga un "Taccuino personale del cittadino", benché "non certificato", in cui il paziente può, comunque, riportare informazioni e/o documenti riguardanti il proprio stato di salute.

Come più volte ribadito nel corso dei capitoli precedenti, sebbene l'attenzione per i contenuti del Fascicolo Sanitario Elettronico sia fondamentale, parimenti essenziale è l'utilizzo di infrastrutture ed architetture che facilitino l'interoperabilità tecnica, semantica ed organizzativa tra i sistemi informativi sanitari; consapevole dell'urgenza e della riflessione scientifica che i summenzionati profili tecnici meritano, il Ministero della Salute avverte che specifici documenti di lavoro verranno in futuro redatti per ottemperare a tali esigenze.

Ai fini della modellazione di strutture informative complesse come "*e-Prescription*" e "*Patient Summary*", esplicito è il richiamo nelle "Linee guida" all'utilizzo dello *standard* "HL7", ed in particolare "*CDA release 2*" (di cui si è già parlato nel "Capitolo II"); per quanto invece concerne l'infrastruttura del FSE, il Ministero della Salute indica, come modello da implementare, l'architettura multi-livello di tipo "*Service Oriented Architecture*", integrata nel "Sistema Pubblico di Connettività", e di tipo distribuito, in cui siano cioè previsti "nodi" di primo e di secondo livello (rispettivamente "nodi regionali" e

[256] Per ciò che concerne la donazione degli organi, le "Linee guida nazionali" ricordano che essa è regolamentata dalla legge n. 91 del 1 aprile 1999 e dal decreto ministeriale dell'8 aprile 2000 (modificato dal D.M. 11 marzo 2008).

"nodi locali"), corrispondenti ai punti di erogazione dei servizi nonché alla gestione e reperimento delle informazioni.

Esaurite le considerazioni concernenti gli aspetti tecnici, successivamente le "Linee guida nazionali" affrontano le questioni giuridiche; un intero capitolo è, infatti, dedicato al tema dei "requisiti di liceità per il trattamento dei dati personali contenuti nel FSE", nel quale sono maggiormente evidenziati gli adempimenti da osservare nei confronti del cittadino ed i suoi diritti. Tra questi rientrano: il dovere di "informativa" da parte del titolare del trattamento[257]; il consenso "esplicito" del paziente alla costituzione del proprio FSE; il "consenso informato al trattamento dei dati", sempre modificabile e revocabile, di tipo c.d. "modulare", cioè specifico sia per la tipologia di documenti da rendere consultabili (di cui possono fare parte quelli antecedenti alla costituzione del FSE personale) sia per i soggetti abilitati ad accedervi; i diritti di "oscuramento" ed "oscuramento dell'oscuramento"[258]; sono altresì garantiti i diritti riconosciuti dall'articolo 7 del "Codice *privacy*".

Parimenti importante è, inoltre, quanto evidenziato dal Ministero della Salute nel capitolo "Definizione di ruoli, profili, e modalità di accesso", soprattutto per ciò che riguarda i temi del presente studio: trattasi dell'organizzazione di tipo modulare basata sulla classificazione dei dati, da prediligere nel *design* del FSE. Tale organizzazione consente di gestire, in modo differenziato, la consultazione delle informazioni sanitarie, accessibili ai soli soggetti autorizzati, in conformità a quanto previsto nelle politiche di accesso, preferibilmente redatte ed efficaci a livello federato tra le Regioni.

Per tutti i motivi esposti in apertura del presente capitolo, anche il tema delle "misure di sicurezza" è oggetto delle "Linee guida nazionali"; in proposito, però, non è introdotta alcuna particolare novità, rispetto a quanto previsto nel decreto legislativo 196/2003 e nel relativo "Disciplinare tecnico (allegato B)", ivi integralmente richiamati.

La parte conclusiva del documento programmatico ministeriale è dedicata agli ulteriori sviluppi che il FSE potrà avere nel contesto italiano, oltre a quelli di prevenzione, diagnosi, cura e riabilitazione; in proposito il Ministero della Salute sottolinea il ruolo importante che i dati sanitari, ovviamente resi anonimi[259], potrebbero rivestire per il settore della salute pubblica.

---

[257] *Ex* articolo 13, d.lgs. 196/2003.
[258] Di cui si è già parlato nell'analisi delle "Linee guida in tema di fascicolo sanitario elettronico e di dossier sanitario" del Garante per la protezione dei dati personali alle quali, pertanto, si rinvia.
[259] Nel rispetto di quanto previsto dall'articolo 11 del d.lgs. 196/2003.

5.4 La recente normativa in materia di sanità digitale e Fascicolo Sanitario Elettronico

A dare forza alle idee progettuali nate nel contesto del Tavolo interistituzionale del 2008 fu per la prima volta, nel settembre 2010, il disegno di legge "Sperimentazione clinica e altre disposizioni in materia sanitaria".

Ai fini del presente lavoro, un particolare interesse suscita l'articolo 14, rubricato "Disposizioni in materia di fascicolo sanitario elettronico", nel quale è riconosciuto il ruolo che il FSE riveste nel supporto della "programmazione, gestione, controllo e valutazione dell'assistenza sanitaria", nonché di "studi e ricerche scientifiche in campo medico, biomedico ed epidemiologico". Rispetto alle previsioni delle "Linee guida in tema di fascicolo sanitario elettronico e di *dossier* sanitario" del Garante per la protezione dei dati personali innanzi esaminate, la norma estende, dunque, la finalità del trattamento dei dati a circostanze non direttamente afferenti lo stato di salute e le cure di uno specifico soggetto, ponendo perciò i presupposti per l'utilizzo di dati sanitari, sia nei contesti regionali sia a livello centrale, ad esempio per motivi di salute pubblica.

Parimenti centrale l'articolo 16, in cui il FSE viene definito come "l'insieme dei dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito".

Il disegno di legge del 2010 fu convertito in legge, con integrazioni, nel 2012, dal decreto legge 158/2012[260]. Gli articoli relativi al FSE vennero, però, stralciati.

5.4.1 I decreti-legge 179/2012 e 69/2013

A distanza di un biennio dal disegno di legge "Sperimentazione clinica e altre disposizioni in materia sanitaria", il Governo italiano dà finalmente luce ad un provvedimento di rango primario, il decreto-legge 18 ottobre 2012 n. 179, convertito in legge alla fine dello stesso anno (c.d. "Provvedimento crescita 2.0"), nel quale sono affrontate alcune tra le questioni maggiormente rilevanti in tema di digitalizzazione dei servizi pubblici nazionali[261]. Tra le misure introdotte dal testo legislativo, di particolare

[260] Decreto-legge 13 settembre 2012 n. 158, pubblicato in G.U. 13.11.2012 n. 214, coordinato con la legge di conversione 8 novembre 2012 n. 189, recante "Disposizioni urgenti per promuovere lo sviluppo del Paese mediante un più alto livello di tutela della salute".

[261] *Cfr*. Decreto-legge 18 ottobre 2012 n. 179, *Ulteriori misure urgenti per la crescita del Paese*, pubblicato in G.U. n. 245 del 19.10.2012 e convertito con legge 17 dicembre 2012 n. 221. Le misure contenute nel provvedimento hanno lo scopo di rendere operativa la "Agenda Digitale Italiana" (ADI), istituita nel marzo 2012 con decreto del Ministro dello sviluppo economico, di concerto con il Ministro per la pubblica amministrazione e la semplificazione, il Ministro per la coesione territoriale, il Ministro dell'istruzione,

interesse per la presente ricerca è la sezione IV dedicata alla "sanità digitale", la quale consta delle seguenti norme: l'articolo 12, rubricato "Fascicolo sanitario elettronico e sistemi di sorveglianza nel settore sanitario"; l'articolo 13, "Prescrizione medica e cartella clinica digitale" nonché l'articolo 13-bis, "Ricetta medica", quest'ultimo integralmente abrogato dalla legge di conversione e modifica 221/2012[262].

A pochi mesi dall'entrata in vigore del "Provvedimento crescita 2.0", il Governo italiano è nuovamente impegnato sul fronte della digitalizzazione dei servizi pubblici; in particolare, per ottemperare alle forti esigenze di crescita economica del Paese viene emanato il decreto-legge 21 giugno 2013 n. 69, "Disposizioni urgenti per il rilancio dell'economia", convertito con legge 9 agosto 2013 n. 98[263]. Nel testo legislativo, noto anche come "Decreto del fare", il capo II è dedicato alle "misure per il potenziamento dell'Agenda digitale italiana"; tra queste, come prevede l'articolo 17, rientrano le "Misure per favorire la realizzazione del Fascicolo sanitario elettronico"[264], norma con cui viene modificato in alcune sue parti l'articolo 12 del d.L. 179/2012.

Tenuto conto dei recenti cambiamenti, per semplicità espositiva sarà di seguito considerato l'articolo 12 nella sua versione vigente.

Il comma I dell'articolo 12 anzitutto definisce il Fascicolo Sanitario Elettronico, inteso come "l'insieme dei dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito"; trattasi, dunque, come già ricordato, non di una cartella clinica, non di una scheda sanitaria, ma di "dati" che, pertanto, devono essere considerati e gestiti come tali (sia dal punto di vista giuridico sia dal punto di vista tecnico).

Se fosse possibile fornire un'iconografia della suddetta definizione, si potrebbe optare per quella di seguito proposta, nella quale predomina il concetto non tanto di documento digitale inteso come "*unicum*", bensì quello di raccolta dinamica di dati, da cui derivano le

---

dell'università e della ricerca e il Ministro dell'economia e delle finanze. Organo operativo dell'ADI è la "cabina di regia", costituita da un gruppo di esperti nominati per l'individuazione di una strategia italiana sul digitale; la valutazione ed il monitoraggio degli obiettivi individuati sono stati affidati alla "Agenzia Digitale Italiana", istituita con decreto legge 22 giugno 2012 n. 83, c.d. "Decreto Sviluppo", pubblicato in G.U. n. 147 del 26.6.2012, convertito, con modificazioni, dalla legge 7 agosto 2012 n. 134, pubblicata in G.U. n. 187 del 11.8.2012.

[262] Legge 17 dicembre 2012 n. 221, *Conversione in legge, con modificazioni, del decreto-legge 18 ottobre 2012, n. 179, recante ulteriori misure urgenti per la crescita del Paese*, pubblicata in G.U. n. 294 del 18.12.2012.

[263] *Cfr*. Decreto-legge 21 giugno 2013 n. 69, *Disposizioni urgenti per il rilancio dell'economia*, coordinato con la legge di conversione 9 agosto 2013 n. 98, pubblicato in G.U. n. 144 del 21 giugno 2013.

[264] *Cfr*. Appendice.

dovute implicazioni concernenti l'architettura dei sistemi informativi e l'apparato normativo (*cfr. fig. 13*).

Figura 13 - Struttura dinamica del FSE

Analogamente a quanto disposto dall'articolo 14 del disegno di legge "Sperimentazione clinica e altre disposizioni in materia sanitaria", e contrariamente a quanto emergeva dalla definizione convenzionale di FSE in cui il trattamento dei dati era ammesso esclusivamente per finalità di prevenzione, diagnosi e cura, il comma II, lettere (b) e (c), dell'articolo 12 del d.L. 179/2012 estende le finalità del trattamento dei dati a motivi di studio e ricerca nonché motivi di salute pubblica. Ovviamente, tale indicazione va letta in combinato disposto con il comma VI, il quale chiarisce che le suddette finalità devono essere perseguite "secondo livelli di accesso, modalità e logiche di organizzazione ed elaborazione dei dati definiti, con regolamento di cui al comma 7, in conformità ai principi di proporzionalità, necessità e indispensabilità nel trattamento dei dati personali".

Tutti i vincoli giuridici previsti dal "Codice *privacy*", quali l'autodeterminazione, l'identificazione, le garanzie sull'accesso nonché il consenso dell'interessato (informato,

autonomo, specifico), sono validati dalla norma in esame, secondo quanto emerge dallo stesso secondo comma.

Un'importante novità introdotta dal decreto-legge è rappresentata dalla funzione attribuita a Regioni e Province autonome, che, ai sensi del comma II, dell'articolo 12, devono istituire il FSE, entro il 31 dicembre 2014; a tal fine, secondo quanto previsto dal comma XV, così come modificato dal c.d. "Decreto del fare", Regioni e Province autonome "possono, nel principio dell'ottimizzazione e razionalizzazione della spesa informatica, anche mediante la definizione di appositi accordi di collaborazione, realizzare infrastrutture tecnologiche per il FSE condivise a livello sovra-regionale, ovvero avvalersi, anche mediante riuso, ai sensi del decreto legislativo 7 marzo 2005 n. 82, delle infrastrutture tecnologiche per il FSE a tale fine già realizzate da altre regioni o dei servizi da queste erogate ovvero avvalersi dell'infrastruttura centrale per il FSE, fruibile in modalità cloud computing e conforme ai criteri stabiliti dal decreto di cui al comma 7, resa disponibile dall'Agenzia per l'Italia Digitale […]".

La previsione legislativa indicata è un chiaro ed inequivocabile segno della volontà di dar vita ad una rete nazionale altamente interoperabile, secondo gli auspici in diverse occasioni espressi dalla Commissione europea, di cui è stata fornita una breve rassegna nel Capitolo Primo della presente ricerca.

Altrettanto significativo il ruolo attivo di cui viene investito l'assistito, il quale partecipa, attraverso le proprie istanze ed il proprio consenso, all'alimentazione continua del FSE[265], perseguita "dai soggetti del Servizio sanitario nazionale e dei servizi socio-sanitari regionali che prendono in cura l'assistito"[266]. Consenso che, in particolare, diviene determinante ai fini della completezza del FSE[267] e delle attività di prevenzione, diagnosi, cura e riabilitazione[268].

Rispetto alla cogenza del testo in esame, parimenti centrale è l'indicazione di cui al secondo comma dell'articolo 12 in merito all'accessibilità ai servizi sanitari *online* da parte

[265] Il comma 3 dell'articolo 12 recita: "3. Il FSE è alimentato in maniera continuativa, senza ulteriori oneri per la finanza pubblica, dai soggetti che prendono in cura l'assistito nell'ambito del Servizio sanitario nazionale e dei servizi socio-sanitari regionali, nonché, su richiesta del cittadino, con i dati medici in possesso dello stesso".

[266] *Cfr*. articolo 12, comma IV, d.L. 179/2012.

[267] Secondo quanto disposto dal comma 3-bis: "Il FSE può essere alimentato esclusivamente sulla base del consenso libero e informato da parte dell'assistito, il quale può decidere se e quali dati relativi alla propria salute non devono essere inseriti nel fascicolo medesimo".

[268] Il comma 5, dell'articolo 12, così dispone: "La consultazione dei dati e documenti presenti nel FSE di cui al comma 1, per le finalità di cui alla lettera a) del comma 2, può essere realizzata soltanto con il consenso dell'assistito e sempre nel rispetto del segreto professionale, salvo i casi di emergenza sanitaria secondo modalità individuate a riguardo. Il mancato consenso non pregiudica il diritto all'erogazione della prestazione sanitaria".

del cittadino attraverso il FSE. Quanto alla consultazione di dati e documenti presenti nel FSE, il comma 6-bis precisa che "può essere realizzata soltanto in forma protetta e riservata secondo modalità determinate dal decreto di cui al comma 7. Le interfacce, i sistemi e le applicazioni software adottati devono assicurare piena interoperabilità tra le soluzioni secondo modalità determinate dal decreto di cui al comma 7". Con i rinvii di cui al comma 7 il legislatore demanda ai ministeri competenti l'individuazione di alcune questione tecniche non di secondaria rilevanza; tra esse: la definizione di limiti di responsabilità e compiti dei soggetti che concorrono alla implementazione del FSE; i sistemi di codifica dei dati, le garanzie e le misure di sicurezza da adottare nel trattamento dei dati personali nel rispetto dei diritti dell'assistito; le modalità e i livelli diversificati di accesso al FSE; i criteri per l'interoperabilità del FSE a livello regionale, nazionale ed europeo, nel rispetto delle regole tecniche del sistema pubblico di connettività etc[269].

5.4.2 Lo schema di decreto sul Fascicolo Sanitario Elettronico attualmente all'esame della Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province Autonome di Trento e Bolzano

Primo dei decreti attuativi previsti dall'articolo 12 del decreto-legge 179/2012, nato per ottemperare alle disposizioni di cui al comma 7 del suddetto articolo e del comma 2-*quater* dell'articolo 13 del decreto-legge 69/2013, attualmente all'esame della Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province Autonome di Trento e Bolzano (previsto all'ordine del giorno del 13 marzo 2014), lo "schema di decreto sul

[269] Il comma VII dell'articolo 12, così recita: "Fermo restando quanto previsto dall'articolo 15, comma 25-bis, di cui al decreto-legge 6 luglio 2012, n. 95, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 135, entro 90 giorni dalla data di entrata in vigore della legge di conversione del presente decreto, ((con uno o più decreti)) del Ministro della salute e del Ministro delegato per l'innovazione tecnologica, di concerto con il Ministro per la pubblica amministrazione e la semplificazione e il Ministro dell'economia e delle finanze, sentita la Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano, acquisito il parere del Garante per la protezione dei dati personali, ai sensi dell'articolo 154, comma 4, del decreto legislativo 30 giugno 2003, n. 196, sono stabiliti: i limiti di responsabilità e i compiti dei soggetti che concorrono alla sua implementazione, i sistemi di codifica dei dati, le garanzie e le misure di sicurezza da adottare nel trattamento dei dati personali nel rispetto dei diritti dell'assistito, le modalità e i livelli diversificati di accesso al FSE da parte dei soggetti di cui ai commi 4, 5 e 6, la definizione e le relative modalità di attribuzione di un codice identificativo univoco dell'assistito che non consenta l'identificazione diretta dell'interessato, i criteri per l'interoperabilità del FSE a livello regionale, nazionale ed europeo, nel rispetto delle regole tecniche del sistema pubblico di connettività".
Il decreto-Legge 21 giugno 2013 n. 69, convertito con modificazioni dalla L. 9 agosto 2013 n. 98, ha modificato il comma VII nella parte ((con uno o più decreti)), disponendo, con l'art. 13, comma 2-quater, che: "I decreti ministeriali previsti dalle disposizioni di cui agli articoli 4, comma 1, 8, commi 2 e 13, 10, comma 10, 12, comma 7, 13, comma 2, e 15, comma 2, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, qualora non ancora adottati e decorsi ulteriori trenta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, sono adottati dal Presidente del Consiglio dei ministri anche ove non sia pervenuto il concerto dei Ministri interessati".

Fascicolo Sanitario Elettronico (FSE)" disciplina: (i) i contenuti del Fascicolo Sanitario Elettronico, (ii) i limiti di responsabilità e i compiti dei soggetti che concorrono alla sua implementazione, (iii) i sistemi di codifica dei dati, (iv) le garanzie e le misure di sicurezza da adottare nel trattamento dei dati personali nel rispetto dei diritti dell'assistito, (v) le modalità ed i livelli diversificati di accesso al FSE, (vi) la definizione e le modalità di attribuzione di un codice identificativo univoco dell'assistito che non consenta l'identificazione diretta dell'interessato.

Il provvedimento si compone di trenta articoli, strutturati in sette capi, nonché di un "Disciplinare Tecnico", allegato ma parte integrante del decreto, nel quale sono definiti: (i) dati identificativi ed amministrativi dell'assistito, (ii) gestione degli accessi, (iii) sistemi di codifica dei dati, (iv) criteri di interoperabilità del FSE a livello regionale, nazionale ed europeo, (v) contenuti del "profilo sanitario sintetico" e del "referto di laboratorio".

Delineate le disposizioni comuni, il legislatore demanda la loro attuazione, così come la realizzazione di infrastrutture tecniche del FSE, a Regioni e Province autonome, nel rispetto del principio costituzionale della ripartizione di competenze in materia di sanità.

Questo elemento potrebbe, tuttavia, svelare le criticità a tutt'oggi esistenti nel panorama nazionale, ancora spesso caratterizzato da un'eterogenea applicazione dei principi di *e-Health* e, dunque, di una lesione sostanziale dei diritti del cittadino (a titolo esemplificativo, vedasi l'articolo 1 che prevede l'alimentazione di "dati e documenti integrativi" del FSE esclusivamente da parte di quelle Regioni con un avanzato processo di digitalizzazione, in conformità con le politiche sanitarie regionali).

Sebbene, infatti, sia pregevole l'intento delle istituzioni governative di muovere la complessa e farraginosa macchina burocratico-amministrativa, consentendo di tradurre a livello territoriale i più alti principi comunitari in materia di sanità digitale, al contempo sono ancora diversi i *gap* culturali, oltre che tecnici, riscontrabili tanto tra gli utenti quanto tra gli operatori (si pensi al tema del *digital divide*).

In questo senso, è auspicabile un intervento congiunto di azioni divulgative e formative che orientino ad un fiducioso utilizzo del FSE, superando, tra le altre, le resistenze su possibili violazioni in materia di trattamento dei dati personali o su rischi elevati di responsabilità medica (in ordine a questo aspetto dispongono, ad esempio, gli articoli 7 e 24, co. 8). Inoltre, rilevanti esempi concernenti tanto il profilo normativo quanto i profili tecnico e architetturale provengono dall'Unione Europea e da alcuni dei 27 Paesi membri con cui l'Italia è chiamata a confrontarsi per trovare forme di armonizzazione.

Secondo quanto previsto dal documento in esame, una valida costituzione del FSE si basa sulla formula del "consenso preventivo", piuttosto che sulla formula del "dissenso esplicito" adottata in altri Paesi europei; gli articoli 7 e 8 precisano che siano rispettivamente ottemperate le norme in materia di informativa e consenso informato, secondo quanto regolato dal "Codice in materia di protezione dei dati personali". In particolare, l'alimentazione del FSE è subordinata al consenso dell'assistito, eventualmente espresso anche in via telematica; parimenti la revoca del consenso implica l'interruzione dell'alimentazione del FSE e la disabilitazione della consultazione dei dati e dei documenti per operatori sanitari e socio-sanitari autorizzati per ragioni di prevenzione, diagnosi, cura e riabilitazione. Nel trattare entrambe le fattispecie astratte, il legislatore ha tenuto presente il rango costituzionale del diritto della salute; per tale motivo, infatti, l'assistito non patisce alcun tipo di conseguenza nella fruizione delle prestazioni a proprio favore e può, in qualsiasi momento, esprimere un nuovo consenso.

Altrettanto tutelati sono, poi, il diritto all'oscuramento e all'"oscuramento dell'oscuramento" (*ex* art. 9, co. 1 e 2): nel primo caso, il titolare del trattamento deve garantire che talune informazioni concernenti lo stato di salute dell'interessato possano non essere visibili dai soggetti autorizzati alla consultazione del FSE; nel secondo è riconosciuto a chi ha esercitato l'oscuramento dei dati l'ulteriore diritto di far sì che non sia visibile, a quanti sono autorizzati all'accesso al FSE, quali informazioni il paziente ha deciso di non divulgare/oscurare.

Eccezioni nell'accesso al FSE per finalità di cura sono previste nell'ipotesi di "accesso in emergenza" (*ex* art. 15).

La possibilità di consultare i dati del FSE è regolata in base ai "ruoli" assunti dalle varie categorie professionali ed è subordinata a forme idonee di autenticazione nonché a "politiche di accesso" federate tra le Regioni e Province autonome (vedasi punto 4 del "Disciplinare Tecnico"). Contrariamente a quanto previsto per la "codifica dei dati", nella sezione dedicata alla "gestione degli accessi" sono affermate solo linee di principio, senza alcun richiamo agli *standard* e/o prassi esistenti a livello europeo e internazionale.

In generale, l'articolato dello "schema di decreto" dichiara conformità alle previsioni di cui al d.lgs. 196/2003, in considerazione del fatto che la natura delle informazioni oggetto del FSE impatta in modo diretto col tema della tutela dei dati personali.

L'articolo 24, rubricato "Misure di sicurezza e sistema di conservazione", è un ulteriore caso che dimostra l'apertura verso il principio della "*Privacy by Design*" (seppur non

espressamente richiamato), caro anche al legislatore comunitario (vedasi la Proposta di "Regolamento generale sulla *privacy*" del 25 gennaio 2012).

Un funzione altrettanto centrale, per ragioni analoghe, è assunto dal "Codice dell'Amministrazione Digitale", per gli aspetti normativi concernenti il procedimento e il fascicolo informatico (art. 41), la riproduzione e conservazione dei documenti (artt. 43 e 44) nonché la continuità operativa (art. 50-*bis*).

Analogamente a quanto accade con le informazioni sanitarie di tipo analogico, anche quelle digitali raccolte nel FSE, se de-identificate e, comunque, nel rispetto dei principi di indispensabilità, necessità, pertinenza e non eccedenza, possono essere utilizzate non soltanto per finalità di diagnosi e cura, ma anche per "finalità di ricerca" (capo III) e "finalità di governo" (capo IV). Notevole interesse suscita il tema degli "usi secondari" dei dati sanitari presenti nel FSE, su cui, però, occorre attendere l'emanazione di ulteriori decreti *ad hoc* (*ex* art. 28, co. 3).

Potrebbero essere utili maggiori chiarimenti su quanto sancito dal comma 3, articolo 21, nella parte in cui dispone che i dati oggetto del trattamento per finalità di governo è necessario siano trattati "in forma individuale" ma in modo tale che sia esclusa l'identificabilità dell'interessato. Secondo parte della dottrina, infatti, l'assegnazione di un "codice identificativo univoco dell'assistito", pur non consentendo l'identificazione diretta dell'interessato, potrebbe comunque sottendere una sua identificabilità. In questo caso, verrebbe violato il Codice *privacy* che considera dati personali sia quelli di identificazione sia quelli di identificabilità.

CAPITOLO IV

LA SFIDA TECNOLOGICA: *SICUREZZA* E *RIUSO* DEI DATI SANITARI

SOMMARIO: 1. I dati al centro dei sistemi informativi sanitari. Elementi essenziali per il miglioramento della salute individuale e collettiva - 2. "*Privacy Enhancing Technology*": origini, evoluzione e principi generali - 2.1 Le "*Privacy Enhancing Technology*" nella visione della Commissione europea - 2.2 "*Privacy Enhancing Technologies*" e *e-Health* - 3. "*Privacy by Design*": origini e principi generali - 3.1 Il modello della "*Privacy by Design*" ed il Fascicolo Sanitario Elettronico - 4. I dati come risorsa per le sfide sociali - 4.1 La risposta italiana al processo di apertura dei dati - 4.2 Gli "*Open Data*" ed i "*Linked Open Data*" come strumento di interoperabilità - 5. Il Fascicolo Sanitario Elettronico come fonte di conoscenza scientifica

1. I DATI AL CENTRO DEI SISTEMI INFORMATIVI SANITARI. ELEMENTI ESSENZIALI PER IL MIGLIORAMENTO DELLA SALUTE INDIVIDUALE E COLLETTIVA

Ciò che in modo costante caratterizza la ricerca fin qui condotta è la presenza di un elemento essenziale per la tutela e la promozione della salute individuale e collettiva: il dato sanitario.

Origine e, al tempo stesso, fine di ogni processo conoscitivo, analogico o digitale, l'informazione sanitaria può rivelarsi decisiva, sia per il singolo utente che si trova al centro dei processi diagnostico-terapeutici, sia per il sistema salute nel suo complesso[270]. Come illustrato in *figura 14*, idealmente potrebbe asserirsi che il dato sulla salute assolve una duplice funzione: cooperare al miglioramento del "benessere fisico, psichico e sociale"[271] del paziente e contribuire all'efficienza/efficacia del sistema sanitario.

Le modalità attraverso cui tali obiettivi possono essere raggiunti sono ovviamente differenti, giacché diversi sono i bisogni dei due attori indicati: mentre nel caso

[270] Significativo evidenziare che il dato, oltre a costituire una fonte di informazione per l'essere umano, può essere oggetto di elaborazione anche di mezzi elettronici. Di questa duplice utilità si tiene particolarmente conto nella presente ricerca, in cui i due profili, umano e tecnologico, sono strettamente connessi proprio per il tipo di conoscenza che è rappresentata nel FSE.

[271] *Cfr. Preamble to the Constitution of the World Health Organization as adopted by the International Health Conference*, New York, 19-22 June, 1946; signed on 22 July 1946 by the representatives of 61 States (Official Records of the World Health Organization, no. 2, p. 100) and entered into force on 7 April 1948. Importante ricordare che la definizione di salute ("*a state of complete physical, mental and social well-being and not merely the absence of disease or infirmity*") adottata da *the International Health Conference* non ha subito alcuna modifica fin dal 1948.

dell'assistito le informazioni idonee a rivelarne lo stato di salute permettono al personale sanitario di porre in essere le azioni necessarie alla cura della persona, nel caso del sistema sanitario, invece, i dati, acquisiti in forma anonima[272] ed aggregata, sono elaborati da esperti e *policy maker* per predisporre azioni e politiche volte al bene comune.

Le osservazioni summenzionate hanno pari valore sia per gli scenari analogici sia per quelli digitali. Con preciso riferimento al contesto digitale vanno, però, formalizzate ulteriori considerazioni che potrebbero così essere sintetizzate: è indispensabile dar vita a sistemi informativi che rispondano congiuntamente ai requisiti di *sicurezza* e *riuso* (*cfr. fig. 14*). Di seguito si annoverano alcune tra le ragioni più significative che giustificano l'affermazione.

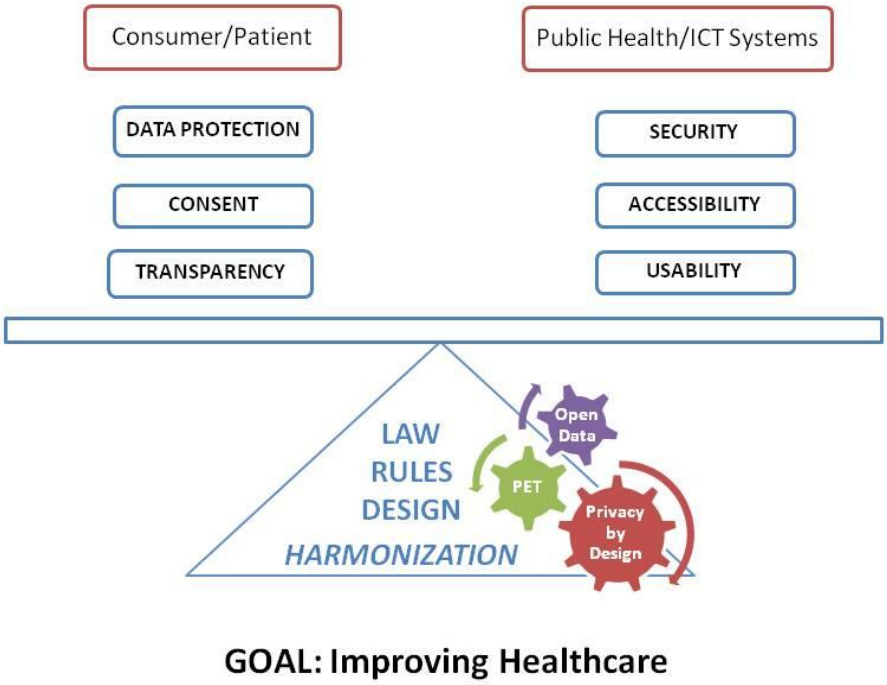


Figura 14 - I dati sanitari come vettore per il miglioramento della salute personale e collettiva

Più volte è emerso dal presente studio che i dati oggetto di sistemi informativi sono esposti a maggiori rischi, in termini di protezione dei dati personali, rispetto a quanto accade con i dati registrati su documenti cartacei. Dal punto di vista del paziente questo aspetto ritrae una criticità: non sempre, infatti, l'utente è disposto a sacrificare la propria

[272] Per approfondimenti sul concetto di anonimato, *cfr*. G. FINOCCHIARO, *voce Anonimato*, in Basile, Sacco, Scala (con la collaborazione di), Digesto delle discipline privatistiche, Iannarelli-Rook, sez. civ., agg., Torino, 2010.

sfera intima, talora anche a costo di mettere in pericolo la propria integrità psico-fisica. Da ciò deriva la necessità di dar vita a norme e prassi che, di fatto, tutelino questo diritto fondamentale ed incoraggino l'adozione di strumenti tecnici idonei ad assolvere tali funzioni.

Altro profilo centrale è, poi, rappresentato dalla possibilità, per i sistemi sanitari centrali (regionali, nazionali, europei), di accedere, fruire ed usare i dati contenuti nei sistemi informativi.

L'acquisizione, in forma anonima, ed il riuso di informazioni per finalità secondarie (come ad esempio, per la ricerca clinica, epidemiologica, farmaceutica etc.) consente di espandere i campi di indagine, sia sotto il profilo qualitativo sia quantitativo[273]. In questo senso, di estremo interesse è la possibilità di realizzare dati sanitari "aperti"[274], non soltanto a partire dalle informazioni già a disposizione del Servizio Sanitario Nazionale nel suo complesso, ma anche di quelle raccolte nei Fascicoli Sanitari Elettronici dei cittadini.

Le recenti previsioni di rango primario, quali i decreti legislativi 179/2012 e 69/2013, che hanno esteso le finalità del trattamento dei dati contenuti nei FSE a motivi di studio e ricerca nonché motivi di salute pubblica, non escludono, anzi, avvalorano l'importanza di usi secondari delle informazioni sanitarie de-identificate[275].

Questo risultato, però, non è scevro di lacune e limiti, soprattutto in un contesto, come quello attuale, caratterizzato da una forte mobilità transnazionale dei cittadini/utenti: in questo contesto, infatti, appare indispensabile una definizione attenta e puntuale di indicazioni riguardanti le modalità di apertura e protezione dei dati nei sistemi e tra i sistemi. A tal fine, è, ad esempio, auspicabile che sia affrontato, con maggiore insistenza, tanto a livello nazionale quanto a livello comunitario, il tema dell'interoperabilità delle *security policy*, e ciò, allo scopo di veicolare, tra le aziende ospedaliere nazionali e quelle presenti nei 27 Paesi membri, una concreta condivisione non soltanto del concetto di sicurezza operante all'interno dei sistemi, ma anche degli obiettivi perseguiti e degli strumenti utilizzati per implementare ambienti operativi sicuri[276]. Parimenti centrale è,

---

[273] In materia di riutilizzo dell'informazione nel settore pubblico vedasi: *Direttiva 2003/98/CE del Parlamento europeo e del Consiglio del 17 novembre 2003* nonché COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI, *Riutilizzo dell'informazione del settore pubblico - Riesame della direttiva 2003/98/CE* -, Bruxelles, 7.5.2009, COM(2009) 212 definitivo.

[274] Ai sensi del comma 3 dell'articolo 68 del "Codice dell'Amministrazione Digitale" (d.lgs. 82/2005), per "formato di dati di tipo aperto" s'intende "un formato di dati reso pubblico, documentato esaustivamente".

[275] Ai decreti del 2012 e del 2013 è stato dedicato un paragrafo nel capitolo "Sistemi informativi e dati personali in sanità elettronica" della presente ricerca.

[276] Ulteriori approfondimenti in tema di *security policy* sono stati forniti nel capitolo III.

inoltre, un rinnovato confronto sulle tecniche di de-identificazione dell'informazione contenuta nei FSE: queste, infatti, non soltanto meritano di essere preferite alle più blande forme di pseudo-anonimizzazione con le quali i rischi di re-identificazione degli interessati sono, certamente, più ampi, ma, soprattutto, è preferibile che siano adottate "*by default*", per una garanzia forte in caso di uso secondario dei dati sanitari[277].

Per concludere. Il potenziale informativo che i dati sanitari hanno in sé stessi è un aspetto che non può essere sottovalutato, ma, che, anzi, va massimizzato, a vantaggio di tutti gli attori coinvolti, seppur nel rispetto delle regole, tecniche e giuridiche, esistenti. Essenziale è, in tal senso, implementare veri e propri "modelli di armonizzazione" di norme, principi e metodologie adottabili non soltanto a livello locale, ma, soprattutto, a livello centrale ed europeo.

Speciale attenzione meritano, a tal fine, le seguenti tematiche, i cui punti di forza e di criticità, nell'ottica della sanità digitale in generale e del FSE in particolare, saranno evidenziati nel corso del capitolo: trattasi delle "*Privacy Enhancing Technology*", della "*Privacy by Design*" e degli "*Open Data*".

Affiancare argomenti così distanti tra loro, sia sotto il profilo giuridico sia sotto il profilo tecnologico, può sembrare incomprensibile. Ancora una volta, però, il punto di convergenza nell'affrontare le suddette questioni va ravvisato nell'idea per cui è indispensabile progettare sistemi informativi sanitari sicuri ed usabili (*cfr. fig. 14*). La *PbD* da una parte e gli "*Open Data*" dall'altra rientrano tra gli strumenti idonei al perseguimento di questi obiettivi: in una prospettiva ideale, infatti, il giurista, l'interprete, il tecnico, il consumatore possono parimenti veder soddisfatti i propri interessi e tutelati i propri diritti.

Come si avrà modo di osservare, per ottenere un tale risultato è fondamentale tener conto dei principi della "*Privacy by Design*" e degli "*Open Data*" già in fase di progettazione e di *design* del Fascicolo Sanitario Elettronico. A tal fine, una specifica attenzione merita l'architettura dei dati che deve rispondere, in modo efficiente ed efficace, alle finalità di tutela delle informazioni personali nonché di accessibilità delle sole informazioni riutilizzabili.

Una nota finale è necessaria. Ci si è interrogati se sia o meno utile considerare la *PbD* e gli *OD* secondo un ordine temporale, sintetizzabile nell'interrogativo: nella progettazione

[277] *Cfr*. A. CAVOUKIAN, R. C. ALVAREZ, *Embedding Privacy into the Design of EHRs to Enable Multiple Functionalities – Win/Win*, 2012, pp. 19; A. CAVOUKIAN, K EL EMAM, *A Positive-Sum Paradigm in Action in the Health Sector*, 2010, pp. 6.

di un sistema informativo, occorre anzitutto pensare in termini di "*Privacy by Design*" o di "*Open Data*"?

Diverse risposte al quesito sono possibili, a seconda che si scelga di valutare o meno l'apertura dell'informazione come obiettivo principale dell'attività di *design*. In questo caso, a livello normativo ed applicativo, occorrerà preferibilmente perseguire una vera e propria "tutela funzionale" degli "*Open Data*".

Nella presente ricerca, la questione è affrontata seguendo una logica differente, non di antitesi ma di sintesi. Se è vero che l'apertura dei dati e il riuso dell'informazione è giuridicamente possibile esclusivamente per i dati pubblici, i principi e gli strumenti per la protezione dei dati personali rappresentano una buona pratica che investe ogni tipo di informazione, tanto quella personale e sensibile, quanto quella de-identificata. Una tutela giuridica *by default* del diritto alla *privacy* favorisce, infatti, processi di utilizzo dei dati in linea con le nuove tecnologie.

2. "*PRIVACY ENHANCING TECHNOLOGY*": ORIGINI, EVOLUZIONE E PRINCIPI GENERALI

Norme e regolamenti, vincolanti e non, comunitari e nazionali, convergono su un punto centrale più volte sottolineato nel capitolo del presente studio dedicato a "Sistemi informativi e dati personali in sanità elettronica": la necessità di predisporre misure di sicurezza idonee alla tutela dei dati personali del cittadino/utente. Tale obiettivo può essere perseguito con diverse modalità, proprio perché molteplici sono le fattispecie concrete che richiedono l'attuazione di appropriate strategie ed efficaci strumenti tecnici. Se ciò è vero per le realtà cartacee, è altrettanto vero per quelle digitali, in cui, oltre ai rischi causati da persone fisiche, autorizzate e non al trattamento dei dati, ulteriori pericoli possono sorgere da errate azioni compiute da *software* e sistemi intelligenti per i motivi più disparati (come, ad esempio, un *design* inadeguato, modalità di programmazione inappropriate o tipologia delle infrastrutture IT non adatte).

Il mutato scenario ha orientato, negli ultimi decenni, *stakeholder* e *policymaker* ad una riflessione analitica sui modelli, tecnici e giuridici, da implementare per raggiungere livelli soddisfacenti, per non dire ottimali, in termini di "*privacy*" e di "*security*"; al centro di questa riflessione trova posto la necessità di custodire, in modo integro, continuo ed esclusivo, le informazioni sensibili dell'utente[278].

[278] Storico il documento ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, Guidelines *on the Protection of Privacy and Transborder Flows of Personal Data*, 1980, in cui OECD individuò i seguenti

Nel 1995, tenendo conto dei summenzionati cambiamenti, dei problemi e delle criticità ad essi collegati, "*the Information and Privacy Commissioner of Ontario*"[279] e "*the Dutch Registratierkamer*"[280] pubblicarono "*Privacy-Enhancing Technologies - A Path to Anonymity*", uno studio volto a dimostrare come la tecnologia possa essere utilizzata per contenere gli abusi di dati personali dei consumatori, attraverso limitazioni d'uso e di trattamento[281].

Dal citato rapporto trae origine il concetto di "*Privacy Enhancing Technology*", inteso come insieme di strumenti, non particolarmente invasivi della sfera privata, attraverso cui modellare i sistemi informativi[282].

I principi chiave su cui si basano le *Privacy Enhancing Technology* sono essenzialmente tre: (i) minimizzazione di raccolta, di utilizzo, di divulgazione e di conservazione dei dati identificativi dei pazienti; (ii) partecipazione e coinvolgimento attivi degli utenti, assicurati, tra l'altro, con l'esercizio di poteri di controllo durante il ciclo di vita dei dati personali trattati; (iii) maggiore sicurezza delle informazioni sensibili, sia sotto il profilo del diritto alla riservatezza sia sotto il profilo dell'integrità dei dati, ottenuta attraverso tecniche di anonimizzazione e di de-identificazione delle informazioni sensibili (*fig. 15*).

---

otto principi come base per la protezione dei dati personali: "Collection limitation, Data quality, Purpose specification, Use limitation, Security safeguard, Openess, Individual Participation, Accountability". Altrettanto interessante il recente studio EUROPEAN COMMISSION, DIRECTORATE-GENERAL JUSTICE, FREEDOM AND SECURITY, *Comparative Study On Different Approaches To New Privacy Challenges, In Particular In The Light Of Technological Developments, Final Report*, Centre for Public Reform, Final final version, 20 January 2010, pp. 59.

[279] Trattasi di un organismo indipendente che, dal 1988, sostiene e promuove il tema della protezione dei dati personali in Ontario (Canada).

[280] Autorità garante per la protezione dei dati personali olandese.

[281] *Cfr.* INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, DUTCH REGISTRATIERKAMER, *Privacy Enhancing Technologies - The Path to Anonymity, Registratiekamer*, The Netherlands, Voll. I-II, 1995.

[282] I concetti di anonimizzazione e de-identificazione dei dati, con specifico riferimento a quanto proposto dalle PET, sono ripresi nello standard ISO/IEC 15408:1999, più strettamente dedicato alla definizione di "*Common Criteria*" per la valutazione della sicurezza dei sistemi informativi.
Per ulteriori apprendimenti sul tema delle PETs si rinvia, tra gli altri a: LONDON ECONOMICS, *Study on the economic benefits of privacy-enhancing technologies (PETs). Final Report to The European Commission DG Justice, Freedom and Security*, London, 2010, pp. 238; D. MARTIN, A. SERJANTOV (edited by), *Privacy Enhancing Technologies, Proceeding of 4° international workshop, PET 2004*, Toronto, May 2004, Berlin, 2004; ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY - COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY, *Working Party on Information Security and Privacy. Inventory of Privacy-Enhancing Technologies (PETs)*, DSTI/ICCP/REG(2001)1/FINAL, 2002, pp. 29; J. BORKING, C. RAAB, *Laws, PETs and Other Technologies for Privacy Protection*, Refereed Article, 2001 (1), The Journal of Information, Law and Technology, http://elj.warwick.ac.uk/jilt/01-1/borking.html ; O. TETTERO, *Intrinsic Information Security: Embedding Security Issues in the Design Process of Telematics Systems*, Technical Report 6, Telematica Instituut, Enschede, The Netherlands, 2000.

Figura 15 - Principi fondamentali delle PET

Quanto detto evidenzia chiaramente come il ruolo delle PET sia complementare, e non sostitutivo, rispetto alle norme in materia di protezione e trattamento dei dati personali, e ciò, dal momento che, in generale, l'imperatività e la cogenza del quadro legislativo sono aspetti ausiliari allo sviluppo ed alla diffusione di tecnologie il più possibile condivise ed armoniche, soprattutto ai fini dell'efficienza e dell'efficacia delle azioni intraprese dagli Stati. In un certo senso, potrebbe asserirsi che la *ratio* delle *Privacy Enhancing Technology* sia quella di tradurre i principi di diritto in specifiche tecniche.

Altra importante caratteristica delle PET è il fatto che non si tratta di prototipi delineati *a priori*; la modellazione di strumenti "*PET oriented*", è, al contrario, affidata alle capacità dei tecnici, i quali sono chiamati a formalizzare prodotti tecnologici che, per questa ragione, non sono di per sé neutri, poiché risentono delle infinite variabili legate all'azione soggettiva ed all'ambiente di applicazione.

Il riconoscimento, se di riconoscimento si possa di fatto parlare, del valore assunto dalle PET non è tardato ad arrivare sul fronte legislativo, dal momento che i principi ispiratori di questo approccio hanno trovato una formale collocazione proprio nella direttiva 95/46/EC. Per citarne alcuni: l'utilizzo di *standard* per la protezione della *privacy* e la minimizzazione della raccolta dei dati personali (*ex* art. 6, parr. 1 (b) e (c)); il perfezionamento di mezzi per l'identificazione, l'autenticazione e l'autorizzazione degli utenti (art. 16); la promozione della c.d. "*pseudo-identity*"; la predilezione di comunicazioni criptate nei canali digitali; l'adozione di sistemi biometrici strumentali all'identificazione degli utenti nonché l'istituzione di autorità di controllo che garantiscano

l'effettivo rispetto delle norme in materia di trattamento dei dati personali (ai sensi dell'articolo 28)[283].

Rilevante è, a questo punto, notare come il legislatore comunitario (lo stesso è accaduto con il legislatore italiano) si riferisca in modo generico ai nuovi strumenti digitali: verosimilmente per non rendere desueto l'atto dispositivo, non sono richiamate o suggerite tecnologie o *standard* determinati. Se da una parte questa scelta è condivisibile proprio per la sua *ratio iuris*, dall'altra va dato atto che essa non crea i presupposti per un'effettiva interoperabilità tecnica, semantica o organizzativa, ad esempio, per quanto concerne il Fascicolo Sanitario Elettronico. Non può, infatti, non rilevarsi l'effettiva distanza tra il dettato giuridico e la prassi. Per tale ragione, la traduzione dei principi della *privacy* e della *security* è oggetto di tavoli di lavoro e gruppi di esperti, coinvolti nello sforzo di armonizzare ora lo stato dell'arte nazionale ora quello comunitario. L'esperienza, di cui si è fornito un rapido *excursus* nel capitolo II, mette in luce, però, dei vuoti, a tutt'oggi rilevanti, conseguenza di un'elevata frammentazione delle iniziative in essere e di un'insufficiente azione di implementazione dei progetti pilota.

Ritornando alle peculiarità delle PET, parimenti significativo è notare come nella medesima circostanza più PET siano perfettamente integrabili, e ciò proprio per la funzionalità che ciascuno di questi strumenti ha rispetto all'obiettivo finale: assicurare un adeguato trattamento dei dati personali e garantire elevati livelli di sicurezza dei sistemi informativi.

Alla fine degli anni Novanta, il concetto di *Privacy-Enhancing Technology* si è evoluto in quello di "*PETs Plus*". Su iniziativa di Ann Cavoukian, "*the Information and Privacy Commissioner of Ontario*", al *design* degli strumenti di ICT è stato idealmente affiancato il c.d. "*positive-sum paradigm*": la novità principale va individuata nella realizzazione di veri e propri modelli inclusivi, in cui tutela dei dati personali del singolo utente ed interessi economici non siano antitetici. In quest'ottica, infatti, la protezione degli uni può rivelarsi rafforzativa della stessa sicurezza dei mercati, a beneficio, dunque, di tutti i soggetti coinvolti e non soltanto, quindi, dei consumatori individuali. Secondo gli auspici di Cavoukian, è essenziale valorizzare la funzione che le infrastrutture e le loro componenti di per sé hanno nella tutela dei dati sensibili, così come è centrale continuare ad implementarne i profili tecnici, per garantire l'efficienza e l'efficacia delle nuove

[283] Nel recepimento della direttiva 95/46/CE, analoghe previsioni sono state introdotte anche nell'ordinamento giuridico italiano, in particolare vedasi *Codice in materia di protezione dei dati personali, Capo II - Misure minime di sicurezza (artt. 33-36) nonché allegato B - Disciplinare tecnico in materia di misure minime di sicurezza*.

tecnologie in termini di *privacy* e *security*. Simili strategie devono, però, agevolare la fiducia degli utenti; soltanto così, infatti, i consumatori saranno incentivati ad adottare tali mezzi elettronici, con un effettivo riscontro positivo sia in termini individuali sia collettivi[284].

Le posizioni teoriche delineate sono state condivise e recepite da un'Unione europea consapevole tanto delle potenzialità quanto delle fragilità sottese allo scenario illustrato.

2.1 LE "*PRIVACY ENHANCING TECHNOLOGY*" NELLA VISIONE DELLA COMMISSIONE EUROPEA

I crescenti rischi per l'identità individuale, conseguenza della rapidità di divulgazione dei dati e della visibilità degli stessi da una pluralità di soggetti, talora, purtroppo, non autorizzati all'accesso, hanno orientato la Commissione europea a sostenere l'utilizzo delle PET, nella consapevolezza, appunto, che l'affermazione di principi giuridici in materia di *privacy* debba essere corredata dall'adozione di misure di sicurezza idonee a garantirli.

Nella "Prima relazione sull'applicazione della direttiva sulla tutela dei dati", già menzionata nel capitolo I, per contribuire al raggiungimento di livelli sufficienti di protezione dei dati personali, la Commissione europea ha evidenziato l'importanza di promuovere ed incoraggiare l'adozione di *Privacy-Enhancing Technology*; in particolare - si sottolinea nel documento - è essenziale che le misure elettroniche, scelte per dare attuazione alla direttiva 95/46/EC, siano "*privacy-compliant*" e "*privacy-friendly*", e, soprattutto, "*privacy-enhancing*". Occorre, cioè, che le tecnologie non soltanto "rispettino" i principi di protezione dei dati personali sovrastanti i sistemi, ma che, anzi, "generino" sistemi informativi fortemente strutturati ed ancorati a tali principi. In questo senso, però, secondo quanto emerge dalla Relazione del 2003 - la cui attualità, a distanza di un decennio, rimane pressoché indiscussa - sono ancora parecchie le difficoltà che gli Stati membri hanno nell'individuare mezzi idonei ed al contempo riconoscibili dagli utenti come sicuri ed affidabili[285]. Tra i campi d'azione individuati dalla Commissione per l'implementazione della direttiva sulla tutela dei dati rientra proprio la promozione delle PET (*cfr*. "*action 8*"), peraltro, già oggetto di significativi progetti pilota quali "RAPID"

[284] *Cfr*. A. CAVOUKIAN, *Moving Forward From PETs to PETs Plus: The Time for Change is Now*, Toronto, 2009, pp. 4; A. CAVOUKIAN, *Privacy by Design … Take the Challenge*, 2009, pp. 361; OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, *7 Essential Steps for Designing Privacy into Technology*, 2002, p. iv. Il paradigma qui richiamato è, peraltro, centrale nella c.d. "Privacy by Design" più avanti affrontata.

[285] *Cfr*. COMMISSIONE DELLE COMUNITÀ EUROPEE, *Prima relazione sull'applicazione della direttiva sulla tutela dei dati (95/46/EC)*, Bruxelles, 15.5.2003, COM(2003) 265 definitivo, pp. 15-16.

(*Roadmap for Advanced Research in Privacy and Identity Management*) e "PISA" (*Privacy Incorporated Software Agent*)[286].

Consapevole dei nuovi rischi e minacce per la tutela dei dati personali, determinati dalla diffusione delle Tecnologie dell'Informazione e della Comunicazione e dalla crescente mobilità internazionale dei consumatori anche verso Paesi terzi, alla luce di quanto sancito dall'articolo 17 della direttiva 95/46/EC e a distanza di un triennio dai risultati emersi dalla "Prima relazione sull'applicazione della direttiva sulla tutela dei dati", nel 2007 la Commissione europea presenta la Comunicazione "sulla protezione dei dati personali attraverso l'utilizzo delle *Privacy Enhancing Technologies* (PETs)", allo scopo di considerare i punti di forza e le modalità di implementazione delle suddette tecnologie, a vantaggio di responsabili del trattamento e consumatori[287].

Richiamati alcuni esempi di tecnologie a favore del potenziamento della *privacy* - tra cui (i) il ripristino automatico dell'anonimato, esauriti gli scopi per i quali i dati sono stati raccolti, (ii) l'adozione di strumenti crittografici e di dispositivi per il blocco dei *cookies* del computer dell'utente, (iii) la condivisione dello *standard* "*Platform for Privacy Preference*" (P3P) per un rilascio, corretto e consapevole, per il trattamento dei dati da parte degli utenti[288] -, la Commissione rinnova il proprio convincimento sull'utilità di adottare *Privacy Enhancing Technology*, per una maggiore efficacia del quadro normativo vigente[289]. I motivi vanno ravvisati nel crescente trattamento di dati personali tramite le reti TIC, nelle quali, come ricordato, i pericoli per la *privacy* sono maggiori, soprattutto per la significativa e diversificata presenza di attori coinvolti; inoltre, la speciale attenzione verso

---

[286] Per ulteriori approfondimenti sul progetto pilota "PISA", vedasi G.W. VAN BLARKOM RE, J.J. BORKING, J.G.E. OLK (eds.), *Handbook of Privacy and Privacy-Enhancing Technologies. The case of Intelligent Software Agents*, PISA Consortium, The Hague, 2003, pp. 372.

[287] COMMISSIONE DELLE COMUNITÀ EUROPEE, *Comunicazione della Commissione al Parlamento europeo e al Consiglio sulla promozione della protezione dei dati mediante tecnologie di rafforzamento della tutela della vita privata (PET)*, Bruxelles, 2.5.2007, COM(2007) 228 def.
Il contenuto della Comunicazione, ed in particolare l'uso delle "*PETs*" e della "*Privacy by Design*", è stato successivamente ribadito in un altro documento europeo, COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, Un approccio globale alla protezione dei dati personali nell'Unione europea*, Bruxelles, 4.11.2010, COM(2010) 609 def.

[288] Lo *standard* "*P3P*", sviluppato da *World Wide Web Consortium* ed ufficialmente raccomandato dal 2002, ha come obiettivo primario aumentare la fiducia degli utenti e la fiducia nel Web attraverso il potenziamento tecnico in materia di "*privacy*". "*P3P*" permette la creazione di un vocabolario comune, a lettura ottica, per identificare pratiche sulla *privacy*; costruito sulla piattaforma *XML*, "*Platform for Privacy Preferences*" favorisce un meccanismo di negoziazione tra *browser* e *server*, che precede la consegna dati. La richiesta di consegna sarà, infatti, approvata ed autorizzata solo se le politiche sulla *privacy* di un sito *web* rispondono ai criteri dello standard "*P3P*" (qualora ci sia una discrasia, l'utente viene informato che le proprie preferenze di privacy non corrispondono a quelle utilizzate dal sito *web*).

[289] Per ulteriori approfondimenti sulle *Privacy Enhancing Technologies*, tra gli altri: I. GOLDBERG, D. WAGNER, E. BREWER, *Privacy-Enhancing Technologies for the Internet*, in Proceedings of IEEE COMPCON '97, 1997, pp. 103-109.

migliori e più adeguati strumenti di *e-Health* va particolarmente rafforzata in un contesto transnazionale, come quello attuale, in cui le giurisdizioni interessate sono varie, sia per numero sia per i principi di diritto affermati[290].

Il raggiungimento dei risultati sperati, secondo il parare della Commissione europea, è possibile anche grazie alle PET, riconosciute come mezzi essenziali per ridurre i pericoli inerenti alle operazioni di trattamento dei dati personali attraverso i canali digitali. Per tale motivo, industrie e piccole e medie imprese da una parte e responsabili del trattamento dei dati[291] e consumatori dall'altra sono incoraggiati a farne uso.

Fondamentale rimane, in questo senso, la definizione tecnica delle PET, per la cui implementazione il 6° (2002-2006) ed il 7° (2007-2013) "Programma quadro per la ricerca e lo sviluppo tecnologico"[292] rappresentano un concreto e significativo impegno da parte dell'Unione europea. Come, infatti, ricordato dalla stessa Commissione, i progetti "PRIME" (*Privacy and Identity Management for Europe*)[293], "OPEN-TC" (*Open Trusted Computing*)[294], "DISCREET" (*Discreet Service Provision in Smart Environments*)[295], così come future iniziative pilota, sono funzionali all'erogazione di "servizi di tutela della *privacy* che responsabilizzino gli utenti, in grado di riconciliare le disparità giuridiche e

[290] Secondo quanto ricordato dalla stessa Commissione nel documento in esame, precisi inviti agli *stakeholder* coinvolti per la realizzazione di sistemi sicuri, erano già stati proposti nella "*Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni, Una strategia per una società dell'informazione sicura - Dialogo, partenariato e responsabilizzazione*", Bruxelles, 31.5.2006, COM(2006) 251 def.

[291] Di cui un significativo esempio è rintracciabile proprio nelle autorità pubbliche, frequentemente coinvolte, nell'era della digitalizzazione, in procedure "a rischio" per il trattamento di dati ed informazioni personali.

[292] *Cfr. Decisione n. 1513/2002/CE del Parlamento europeo e del Consiglio, del 27 giugno 2002, relativa al sesto programma quadro di azioni comunitarie di ricerca, sviluppo tecnologico e dimostrazione volto a contribuire alla realizzazione dello Spazio europeo della ricerca e all'innovazione (2002-2006)*, pubblicata in G.U. L 232 del 29.8.2002 e *Decisione 1982/2006/CE del Parlamento europeo e del Consiglio, del 18 dicembre 2006, concernente il settimo programma quadro della Comunità europea per le attività di ricerca, sviluppo tecnologico e dimostrazione (2007-2013)*, pubblicata in G. U. L 232 del 29.8.2002.

[293] Coordinato da "*International Business Machines Belgium Sa*", il progetto "PRIME" (2004-2008) è nato dalla consapevolezza del crescente divario tra legislazione e prassi nella Rete in materia di *privacy* e dal bisogno dei cittadini europei di mantenere autonomia e controllo sulle proprie informazioni personali. Obiettivo finale del Progetto è, dunque, quello di costruire una sinergica collaborazione nei settori della ricerca, dello sviluppo e della valutazione di soluzioni di "*privacy-enhancing identity management*" (IDM) a beneficio degli utenti finali. Il Portale del Progetto è consultabile all'indirizzo https://www.prime-project.eu/.

[294] "OPEN-TC" è un progetto di ricerca rivolto allo sviluppo di sistemi informatici sicuri; l'implementazione di un software open source è lo strumento attraverso cui "OPEN-TC" intende raggiungere questo risultato. L'homepage del sito dedicato al Progetto è disponibile all'indirizzo http://www.opentc.net/.

[295] Scopo del Progetto "DISCREET" (2005-2008) è ridurre e controllare la quantità di informazioni personalizzate messe a disposizione delle organizzazioni coinvolte, a garanzia e beneficio degli utenti finali. Ulteriore obiettivo è lo sviluppo di tecnologie e soluzioni impiegate in ambienti intelligenti, quali LAN senza fili (WLAN), *Radio Frequency IDentification* (RFID) e reti di sensori. Ulteriori informazioni sono accessibili all'indirizzo http://www.ist-discreet.org/.

tecniche nel territorio europeo attraverso partenariati pubblico/privato"[296].

A distanza di quasi un decennio dalla loro prima concettualizzazione, però, le "*Privacy-Enhancing Technology*" non sono ancora state del tutto sviluppate in molti settori, tra cui, certamente, quello sanitario; da ciò deriva l'attualità della tematica in esame nonché l'importanza di conoscerne profili strutturali e argomenti controversi.

Tra le questioni ancora aperte rientra la necessità di un'armonizzazione tra il livello teoretico/normativo ed il livello pratico/di *design*; parimenti importante definire le modalità di realizzazione di sistemi informativi che incorporino i principi in materia di *privacy* nonché i criteri da utilizzare per la valutazione e la verifica di sistemi così realizzati. Non di secondaria rilevanza, infine, il tema dell'educazione dei consumatori sull'impiego delle nuove tecnologie e sui loro potenziali benefici per il raggiungimento di diversi risultati. Confermano quanto delineato i documenti della Commissione europea in materia di protezione dei dati personali, richiamati tanto nel capitolo I quanto nel presente capitolo.

2.2 "*PRIVACY ENHANCING TECHNOLOGY*" E *E-HEALTH*

Analogamente a quanto riscontrato per il tema della protezione dei dati personali, in cui specifici provvedimenti sono stati delineati da Governi ed autorità competenti su dati sensibili e sanitari, anche il dibattito sulle PET si è esteso all'ambito della sanità digitale[297].

Nella "Raccomandazione della Commissione sull'interoperabilità transfrontaliera dei sistemi di cartelle cliniche elettroniche"[298], in riferimento alla progettazione di sistemi dedicati ai fascicoli sanitari elettronici, la Commissione ha particolarmente incoraggiato gli Stati membri all'uso di "*Security and Privacy Enhancing Technology*", al fine di fronteggiare "il rischio che le informazioni sui pazienti vengano accidentalmente rese

[296] COMMISSIONE DELLE COMUNITÀ EUROPEE, *Comunicazione della Commissione al Parlamento europeo e al Consiglio sulla promozione della protezione dei dati mediante tecnologie di rafforzamento della tutela della vita privata (PET)*, p. 6.

[297] Tra le iniziative promosse nel settore sanitario si ricordano: "*Hippocratic Database*", sviluppato presso *IBM's Almaden Research Centre* e basato sui seguenti dieci principi guida: "*purpose specification, consent, limited collection, limited use, limited disclosure, limited retention, accuracy, openness, and compliance*"; "*Dutch HIS (Hospital Information System*)", in cui sono state recepite le indicazioni della Commissione europea circa l'uso di PETs nei sistemi informativi sanitari; "*IBM's Zurich Research Laboratory*", all'interno del quale, nel 2001, è stato istituito "*IBM Privacy Research Institute*", allo scopo di sviluppare tecnologie *privacy-enhancing* per le imprese.

[298] COMMISSIONE DELLE COMUNITÀ EUROPEE, *Raccomandazione della Commissione del 2 luglio 2008 sull'interoperabilità transfrontaliera dei sistemi di cartelle cliniche elettroniche, notificata con il numero C (2008)3282, 2008/594/CE*, pubblicata in G.U. L 190/37 del 18.7.2008.

pubbliche o facilmente distribuite a persone non autorizzate"[299].

La prospettiva di interoperabilità dei sistemi di cartelle cliniche elettroniche, auspicata nella Raccomandazione del 2008, non ignora, al contempo, che i sistemi informativi sanitari transnazionali operano all'interno di sistemi giuridici nazionali, in cui, modalità di conservazione e, soprattutto, di trattamento dei dati (personali e sanitari) sono frequentemente tra loro difformi[300]. A parere della Commissione, l'attività di collaborazione tecnica sul fronte dell'interoperabilità deve, pertanto, essere coadiuvata da azioni economiche e legislative concrete, tra cui rientra la definizione di "un quadro giuridico completo per i sistemi interoperabili di cartelle cliniche elettroniche" idoneo a fornire elevate garanzie ai pazienti, ad esempio in termini di diritto all'autodeterminazione ed all'anonimato o di minimizzazione nel trattamento dei dati sanitari (*cfr*. paragrafi 14 e 15).

Parimenti significativo è, poi, l'accento posto dalla Commissione sui temi della valutazione dei rischi sulla sicurezza delle informazioni e dell'impatto sulla protezione dei dati personali nel caso di progettazione ed implementazione di sistemi informativi sanitari nonché dei limiti della "messa in Rete" delle informazioni concernenti lo stato di salute.

Non mancano, inoltre, i riferimenti alle modalità di accesso ai dati da parte dei soggetti autorizzati, alla necessità di informativa per i pazienti nonché all'affidabilità richiesta per sistemi di identificazione e riconoscimento elettronici, registrazione dell'accesso ai dati, documentazione delle fasi del trattamento, periodo di mantenimento delle informazioni, meccanismi efficaci di *back-up* e recupero dei dati.

Infine, nell'affrontare le problematiche connesse alla protezione dei dati personali in riferimento ai sistemi di cartelle cliniche elettroniche e nell'individuare possibili strumenti volti a gestirle, la Commissione suggerisce "l'immissione sul mercato di prodotti, processi e servizi volti a migliorare la sicurezza, per impedire e combattere il furto di identità e altre minacce alla vita privata" nonché, appunto, l'uso delle PET nella ideazione ed esecuzione delle applicazioni di amministrazione elettronica.

[299] Ivi, "Considerando n. 10".
[300] Da cui la proposta di un regolamento generale sulla protezione dei dati del 25 gennaio 2012, già ricordata nel capitolo III della presente ricerca.

3. LA "*PRIVACY BY DESIGN*": ORIGINI E PRINCIPI GENERALI

Ispirata al concetto di "*Privacy-Enhancing Technology*", l'espressione "*Privacy by Design*" (PbD) è stata coniata, negli anni Novanta, da Ann Cavoukian[301]. Da allora, e fino alla "*32nd International Conference of Data Protection and Privacy Commissioners*" del 2010[302], in occasione della quale la "*Privacy by Design*" fu formalmente riconosciuta come "*global privacy standard*", su diversi fronti è stata confermata l'importanza di questo *framework*, nel quale è centrale il ruolo che le componenti tecnico-informatiche hanno ai fini della tutela dei dati personali[303].

Ann Cavoukian ha sinteticamente illustrato il concetto di "*Privacy by Design*" attraverso "*The 7 Foundational Principles*" (2002): "1. *Proactive not Reactive*; 2. *Preventative not Remedial*; 3. *Privacy as the Default*; 4. *Privacy Embedded into Design*; 5. *Full Functionality: Positive-Sum, not Zero-Sum*; 6. *End-to-End Lifecycle Protection*; 7. *Visibility and Transparency*; 8. *Respect for User Privacy*"[304].

Un approccio "*Privacy by Design*" può apportare - secondo Cavoukian - evidenti benefici al mercato ("*Privacy is good for business*"); esso, però, richiede anzitutto il rispetto di una pratica universale: l'utilizzo di prassi informative corrette[305].

---

[301] La necessità di sistematizzare "buone pratiche" sul fronte della tutela dei dati personali è alla base dei seguenti due studi, propedeutici alla creazione di questo nuovo "*framework*": OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, *Privacy Protection Makes Good Business Sense*, 1994 e OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, *Privacy: The Key to Electronic Commerce*, 1998. Altrattanto importante il documento OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, *Smart, Optical and Other Advanced Cards: How to Do a Privacy Assessment*, 1997, in cui la metodologia della "PbD" è presentata come "*right from the start*".
Per ulteriori approfondimenti sul tema, si rinvia a: A. CAVOUKIAN, *Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era*, in G. O.M. YEE, Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards, IGI Global, Hershey, 2012, pp. 170-208; A. CAVOUKIAN, *Privacy by Design … Take the Challenge*, 2009, pp. 361; OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, *7 Essential Steps for Designing Privacy into Technology*, 2002; A. CAVOUKIAN (presentation by), *Privacy by Design: Building Trust into Technology, 1st Annual Privacy and Security Workshop. Centre for Applied Cryptographic Research*, Toronto, 2000; OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, REGISTRATIERKAMER THE NETHERLANDS, *Intelligent Software Agents: Turning a Privacy Threat into a Privacy Protector. Result of a joint project of the Office of the Information and Privacy Commissioner/Ontario and the Registratierkamer, The Netherlands*, 1999.

[302] *Cfr*. 32ND INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS, *Resolution on Privacy by Design, Jerusalem - Israel*, 27-29 October 2010.

[303] Secondo quanto affermato dalla stessa "*Information and Privacy Commissioner of Ontario*", settori di applicazione della *PbD* sono: "*1) IT systems; 2) accountable business practices; and 3) physical design and infrastructure*".

[304] *Cfr*. A. CAVOUKIAN, *Privacy by Design. The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices*, Toronto, 2010, pp. 12.

[305] Cavoukian evidenzia l'importanza, in tal senso, de "*The 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*".

Secondo il paradigma, tanto gli enti pubblici quanto gli enti privati sono sollecitati a ripensare, individualmente e collettivamente, la *privacy* seguendo un approccio "proattivo" e "preventivo", che anticipi ed eviti i possibili rischi ai quali i dati sono esposti; le suddette organizzazioni sono, in particolare, invitate ad introdurre la *privacy* "*by default*" nella progettazione di sistemi IT e processi informatici, a vantaggio di una riduzione/eliminazione di interventi architetturali successivi. Grazie a questo meccanismo, i dati dell'utente sono salvaguardati "*a priori*" dai sistemi stessi, senza, dunque, la necessità di interventi attivi da parte degli interessati[306].

Al modello proposto è, altresì, sottesa una visione "*positive-sum win-win*", in cui predomina la riduzione di possibili false dicotomie, come quelle tra *privacy* e *security*, che, al contrario, in questa logica, sono da intendere non come componenti antitetiche ma come aspetti complementari nell'implementazione dei sistemi informativi[307].

Ulteriore caratteristica di sistemi informativi concepiti secondo il paradigma della "*Privacy by Design*" è quella di preservare i dati sensibili lungo l'intero ciclo di vita. Gli interessi del singolo, persona fisica o giuridica, consumatore o ente pubblico/privato, paziente o azienda sanitaria, sono, in questo senso, conciliati.

Inoltre, come più volte ricordato, in questa prospettiva il consumatore assume un ruolo centrale, non soltanto in quanto beneficiario finale delle misure considerate, ma anche in quanto artefice del rispetto della *privacy*, grazie a strumenti "*privacy-friendly*" a lui disponibili.

Soffermandosi sulla "*Privacy by Design*", il commissario federale tedesco per la protezione dei dati e per la libertà dell'informazione, Peter Schaar, ha opportunamente osservato che l'idea di provvedere alla protezione dei dati personali trattati da sistemi informativi attraverso l'utilizzo di tecnologie appropriate è già espressa nella direttiva 95/46/CE; il fine per il quale essa è introdotta è quello di garantire la sicurezza[308]. Con la

---

[306] Secondo quanto, infatti, sostenuto dalla stessa Cavoukian: "*Privacy by Design refers to the philosophy and approach of embedding privacy into the design specifications of various technologies. This may be achieved by building the principles of Fair Information Practices [come "1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*" e "*Global Privacy Standard Privacy Principles" del 2006] into the design, operation and management of information processing technologies and systems*" (in A. CAVOUKIAN, *Privacy by Design … Take the Challenge*, cit., p. 3).

[307] Sul tema della convergenza di paradigma tra la "*Privacy by Design*" e la c.d. "*Security by Design*" (in G. KREIZMAN, B. ROBERTSON, *Incorporating Security into the Enterprise Architecture Process*, Gartner, 2006) vedasi: A. CAVOUKIAN, M. CHANLIAU, *Privacy and Security by Design: A Convergence of Paradigms*, Toronto, 2013, pp. 19.

[308] Il "considerando 46" della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati così recita: "considerando che la tutela dei diritti e delle libertà delle persone interessate relativamente al trattamento di dati personali richiede l'adozione di adeguate misure tecniche ed

PbD, invece, si va oltre: alla sicurezza dei singoli, infatti, si aggiunge l'evitare o, in ogni caso, il ridurre al minimo il trattamento di dati personali a mezzo dei sistemi informativi[309]. La "*data minimization*" è, infatti, secondo Schaar così come secondo altri autori, il nodo centrale in tema di PbD, dal momento che consente un'effettiva riduzione dei rischi per la *privacy*[310].

Pensare, dunque, in termini di "*Privacy by Design*" significa, in un certo senso, "riassegnare" alla *privacy* il ruolo che le è proprio; la protezione ed il trattamento dei dati personali devono, dunque, essere al centro del *design* dei sistemi. Idealmente andrà superato anche il principio della sicurezza, sebbene questo costituisca presupposto o, comunque, pre-requisito della *PbD*. A tal fine, il suddetto paradigma incoraggia, in generale, un vero e proprio meccanismo di prevenzione, raggiungibile, tra gli altri, attraverso la separazione tra identificazione personale e contenuto dei dati stessi, l'uso di pseudonimi e di tecniche di anonimizzazione nonché l'eliminazione dei dati personali in tempi rapidi.

La teorizzazione di qualsiasi modello richiede, però, una lettura critica, al fine di cogliere aspetti positivi ed eventuali limiti sottesi. In proposito risultano interessanti le osservazioni di Pagallo[311], il quale, in un certo senso, propone una lettura ristretta della PbD, a suo dire più compatibile con i profili tecnici, etici e giuridici. Tale soluzione nasce da alcune criticità individuate dal giurista ne "*The 7 Foundational Principles*" di Cavoukian: a) le difficoltà, anzitutto, nella creazione di sistemi neutri, improntati ad una logica "*privacy zero-sum*" e ciò, dal momento che, a parere di Pagallo, è impossibile operare una protezione dei dati in modo automatico, scevra cioè dell'intervento dei

---

organizzative sia al momento della progettazione che a quello dell'esecuzione del trattamento, in particolare per garantirne la sicurezza ed impedire in tal modo qualsiasi trattamento non autorizzato; che spetta agli Stati membri accertarsi che il responsabile del trattamento osservi tali misure; che queste devono assicurare un adeguato livello di sicurezza, tenuto conto delle conoscenze tecniche e dei costi dell'esecuzione rispetto ai rischi che i trattamenti presentano e alla natura dei dati da proteggere".

[309] "*It is very important to examine early in the planning process whether and how to limit the amount of personal data to the absolute minimum necessary. The tendency to reproduce increasingly complicated bureaucratic systems exactly in information technology […] can lead to major problems for data protection*" in P. SCHAAR, *Privacy by Design, Identity in Information Society*, 2010, 3:267-274.

[310] Su questo tema, e, in particolare, su una reingegnerizzazione dei sistemi informativi fondata sul principio della "minimizzazione dei dati" è lo studio S. GÜRSES, C. TRONCOSO, C. DIAZ, *Engineering Privacy by Design, in Conference of Computers, Privacy & Data Protection*, 2011, pp. 25.

[311] *Cfr*. U. PAGALLO, *On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law,* in S. Gutwirth et al. (eds.), European Data Protection: In Good Health?, Springer Science+Business Media B.V, 2012, pp. 331-346. Si veda inoltre, U. PAGALLO, *Privacy e Design,* in M. Pietrangelo (a cura di), Diritti di libertà nel mondo virtuale della rete, Fascicolo monografico di Informatica e diritto, 2009, 1, pp. 123-134 nonché U. PAGALLO, *Designing Data Protection Safeguards Ethically*, in Information, 2011, 2, pp. 247-265 e U. PAGALLO, E. BASSI, *The Future of EU Working Parties' "The Future of Privacy" and the Principle of Privacy by Design*, in M. Bottis (eds.), An Information Law for the 21st Century, Atene, Nomiki Bibliothiki, 2011, pp. 286-305.

responsabili del trattamento dei dati; b) la presenza di una dicotomia tra la libertà di scelta individuale e la sua compressione ad opera di terzi (seppur nel presunto interesse collettivo); c) la possibile lesione del diritto individuale all'autodeterminazione, a seguito del prevaricare di forme automatiche nella protezione dei dati. Sebbene i rischi evidenziati, Pagallo riconosce però la consistenza del concetto di "*positive sum*" o "*win-win game*" nel quale, aboliti i falsi conflitti tradizionali come, ad esempio, quello tra *privacy* e *security*, l'*empowerment* del consumatore assume un ruolo vitale.

3.1 IL MODELLO DELLA "*PRIVACY BY DESIGN*" ED IL FASCICOLO SANITARIO ELETTRONICO

L'analisi condotta consente di trarre alcune conclusioni relative al rapporto tra protezione dei dati personali, sicurezza dei sistemi, diritto alla salute e Fascicolo Sanitario Elettronico. Come rappresentato in *figura 14*, esistono molteplici equilibri di cui è necessario tenere conto, è ciò, considerata la complessità che lo scenario sanitario, come altri settori del resto, presenta: gli interessi, i bisogni, i diritti in gioco sono non soltanto cospicui ma, frequentemente, antitetici. Occorre, dunque, agire adottando un vero e proprio bilanciamento di diritti: quelli del paziente, principale fruitore dei servizi sanitari nonché quelli di tutti gli *stakeholder* direttamente o indirettamente coinvolti nell'erogazione delle varie forme di assistenza; di non secondaria importanza, lo sviluppo crescente di modelli di *business* anch'essi, in un certo senso, attori dei sistemi sanitari.

Per queste ragioni, si ritiene che i principi della "*Privacy by Design*" rappresentino uno strumento essenziale nel contemperamento di tutti gli interessi summenzionati; in particolare, se efficacemente tradotti, tali principi contribuiscono a creare modelli di prevenzione nella tutela della *privacy*. La "*data minimization*", la separazione tra identificazione e contenuto dei dati, l'uso di pseudonimi e di tecniche di anonimizzazione, la cancellazione dei dati personali in tempi brevi sono tutti esempi concreti da utilizzare nel *design* di sistemi informativi e, specialmente, nel *design* del FSE[312].

Affinché la "*privacy by default*" diventi prassi, è, però, centrale creare un vero e proprio *framework* giuridico e tecnologico comunitario, vincolante per gli Stati membri, per: (i)

[312] La fattibilità nel recepire ed adattare i principi della PbD al settore sanitario, ed in particolare, al FSE, trova una concreta manifestazione nella piattaforma canadese "PHEMI Health System" che, utilizzando i dati dei pazienti, persegue gli obiettivi di migliorare la produttività clinica, i risultati per i pazienti e la ricerca medica. Designata nel 2013 da Cavoukian come "azienda ambasciatrice della *Privacy by Design*", PHEMI, infatti, incorpora nelle definizione delle proprie tecnologie *privacy* e *security*. La *homepage* dell'azienda è raggiungibile all'indirizzo http://www.phemi.com/.

l'armonizzazione delle norme esistenti in materia di protezione dei dati sanitari, (ii) l'armonizzazione delle regole tecniche e giuridiche in uso (tra cui rientrano le *security policy*), (iii) l'armonizzazione del *design* degli strumenti informatici e tecnologici (*cfr. fig. 1*).

In questo contesto si colloca, ad esempio, il processo di revisione della direttiva 95/46/CE, avviato il 25 gennaio 2012, ed ancora in essere, da parte della Commissione Europea con la proposta della "*General Data Protection Regulation*", il cui obiettivo è, appunto, armonizzare le regole esistenti in materia di trattamento dei dati personali in accordo con i progressi tecnologici e i nuovi metodi di collezione, accesso ed utilizzo dei dati. La Commissione è, infatti, convinta che la protezione dei dati personali del cittadino sia un diritto fondamentale e che, al contempo, la libera circolazione dei dati personali sia un bene comune[313].

4. I DATI COME RISORSA PER LE SFIDE SOCIALI

I dati, secondo quanto affermato nel "*Digital Britain Report*"[314] del 2009, rappresentano "una valuta innovativa" e la "linfa vitale dell'economia della conoscenza". Per tale motivo, sottolinea la Commissione europea, un loro "trattamento intelligente è essenziale per affrontare le sfide sociali" (quali, ad esempio, la "sostenibilità dei sistemi sanitari nazionali") o "per accelerare il progresso scientifico" (l'*e-science*, infatti, grazie a maggiori quantitativi di dati può intraprendere nuove piste di ricerca)[315]. Benefici di politiche ed azioni che abbiano come fondamento tale idea, sono, dunque, rivolti ai cittadini, alla società, all'economia, alla scienza, al settore pubblico nel suo insieme, alla stessa democrazia[316].

Le suddette considerazioni avvalorano la tesi sostenuta all'inizio del capitolo secondo cui il dato digitale sanitario de-identificato, per le sue diverse funzioni, va tenuto al centro

[313] Unitamente alla *privacy by default*, la riforma della legislazione sulla protezione dei dati intende rafforzare alcuni diritti dei cittadini, tra questi, a titolo esemplificativo, si ricordano il diritto all'oblio, il diritto ad una più facile trasferibilità dei dati tra *service provider*, il diritto al controllo sui propri dati.

[314] THE DEPARTMENT FOR CULTURE, MEDIA AND SPORT AND THE DEPARTMENT FOR BUSINESS, INNOVATION AND SKILLS, *Digital Britain - Final Report*, 2009, London, The Stationery Office, pp. 238.

[315] *Cfr.* COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI, *Dati aperti. Un motore per l'innovazione, la crescita e una governance trasparente*, Bruxelles, 12.12.2011, COM(2011) 882 def. Esempi di informazioni importanti ricordati dalla Commissione nella citata Comunicazione sono altresì: "le informazioni geografiche, le statistiche, i dati meteorologici, i dati acquisiti in progetti di ricerca a finanziamento pubblico e i libri digitalizzati delle biblioteche".

[316] Come evidenziato da Neelie Kroes, vice Presidente della Commissione europea, responsabile per l'Agenda digitale, durante l'*OpenForum Europe Summit* del 2011.

di politiche ed azioni rivolte tanto all'interesse del singolo quanto all'interesse della collettività (*cfr. fig. 1*)[317].

A questo punto, però, è bene ricordare che, storicamente, l'attenzione dei *policy maker* verso l'apertura e l'accessibilità dei dati non ha avuto origine dal settore sanitario (ove la presenza di informazioni personali e sensibili è ovviamente elevata), bensì dal più ampio e generico contesto dell'informazione pubblica (*Public Service Information - PSI*) in senso stretto. Parimenti si può, tuttavia, ritenere che, per i motivi che si diranno, non vi sia incompatibilità o, comunque, impossibilità di estendere anche al FSE le osservazioni in materia di riutilizzo ed apertura dei dati, seppur con i dovuti accorgimenti in riferimento alla protezione delle informazioni personali e sensibili.

L'interesse per la *PSI*, così come per i principi di trasparenza amministrativa, di partecipazione collettiva e di collaborazione tra gli *stakeholder* (istituzioni, ONG, cittadini etc.) ad oggi permangono, sia a livello internazionale sia a livello comunitario e nazionale[318]. In particolare, il riutilizzo, commerciale e non commerciale, di dati pubblici, diffusi in modo "grezzo"[319] e fruibili in "formati aperti"[320], nel rispetto del diritto alla riservatezza[321] e della proprietà intellettuale[322], rientra tra le idee portanti della strategia decennale "Europa 2020", della Agenda digitale europea[323] e, prima ancora, del processo

---

[317] Parimenti importante è a tal fine richiamare la seguente osservazione di cui alla Comunicazione (2011) 882, par. 2.2: "progressi in settori quali la genomica, la scoperta di farmaci, la diagnosi e il trattamento di malattie gravi quali il cancro o le malattie cardiovascolari, dipendono sempre di più dalle tecniche di raccolta e analisi di dati sofisticati".

[318] *Cfr*. B. OBAMA, *Transparency and Open Government, Memorandum for the Heads of Executive Departments and Agencies*, 2009, consultabile all'indirizzo http://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment. Tra gli interventi normativi comunitari e nazionali più rilevanti in questo settore, si ricordano: *Direttiva 2003/98/CE del Parlamento europeo e del Consiglio, del 17 novembre 2003, relativa al riutilizzo dell'informazione del settore pubblico*, pubblicata in G.U. del 31.12.2003, D.lgs. 24 gennaio 2006 n. 36, *Attuazione della direttiva 2003/98/CE relativa al riutilizzo di documenti nel settore pubblico*, pubblicato in GU. n. 37 del 14.02.2006; *Direttiva n.8/2009 del Ministro per la Pubblica Amministrazione e l'Innovazione, per la riduzione dei siti web delle Pubbliche Amministrazioni*, e "*Linee guida per i siti web della PA*" allegate; D.lgs. 7 marzo 2005 n. 82, *Codice dell'amministrazione digitale*, pubblicato in G.U. n. 112 del 16.05.2005 e successive modifiche.

[319] Con l'espressione "*raw data*" si fa riferimento ai dati raccolti che non hanno subito alcuna modifica, manipolazione o aggregazione.

[320] La medesima indicazione vale per i "metadati" dei documenti in possesso degli enti pubblici (così dispone l'articolo 5, par. 1, della *Direttiva 2003/98/CE del Parlamento europeo e del Consiglio del 17 novembre 2003 relativa al riutilizzo dell'informazione del settore pubblico, così come modificata dalla Direttiva 2013/37/UE del Parlamento europeo e del Consiglio del 26 giugno 2013*).

[321] Per approfondimenti, tra gli altri vedasi: E. BASSI, *PSI, protezione dei dati personali, anonimizzazione*, in Informatica e diritto, ESI Italiane, Napoli, fasc. 1-2, 2011, pp. 65-84; B. VAN DER SLOOT, *Public Sector Information & Data Protection: A Plea for Personal Privacy Settings for the Re-use of PSI*, in Informatica e diritto, ESI, Napoli, fasc. 1-2, 2011, pp. 219-238.

[322] Di interesse sul tema: A. M. ROVATI, *Prime note su proprietà intellettuale e riutilizzo dei dati pubblici, in Informatica e diritto*, ESI, Napoli, fasc. 1-2, 2011, pp. 153-184; C. SAPPA, *Diritti di proprietà intellettuale e dati pubblici nell'ordinamento italiano*, in Informatica e diritto, ESI, Napoli, fasc. 1-2, 2011, pp. 185-198.

[323] I citati documenti europei sono già stati esaminati per gli aspetti di interesse nel capitolo I del presente studio.

di ammodernamento della P.A. (noto anche come *e-Government*[324]). Le ragioni di un così vivo interesse sono essenzialmente da attribuire al fatto che il riuso può contribuire in modo essenziale allo sviluppo del mercato comunitario, in quanto generatore di prodotti e servizi imperniati proprio su contenuti digitali in possesso di enti pubblici nazionali o organismi di diritto pubblico. Tale realtà è vivamente sentita negli ultimi anni, durante i quali la grave crisi economica sta orientando i decisori pubblici verso una nuova modernizzazione e trasformazione della P.A. mediante l'uso delle Tecnologie dell'Informazione e Comunicazione; ne sono, tra gli altri, significativa dimostrazione il "Piano d'azione collettivo dei Paesi del G8"[325] ed il nuovo Programma Quadro europeo per la Ricerca e l'Innovazione "*Horizon 2020*"[326].

Nonostante da circa un decennio il tema del riutilizzo dell'informazione pubblica per garantire il più ampio uso possibile delle risorse di dati sia oggetto di attenzione da parte del legislatore comunitario e nonostante ne siano riconosciuti benefici ed opportunità economiche, tuttavia, tra i 27 Paesi membri sono ancora presenti criticità pregiudizievoli per i diritti dei cittadini europei, sia di carattere giuridico sia tecnologico, sinteticamente rintracciabili in una mancanza di armonizzazione tra legislazioni e prassi nazionali.

Per superare tali ostacoli, l'Unione europea ha avviato interventi mirati, allo scopo di: (i) rivedere la direttiva 2003/98/UE relativa al riutilizzo dell'informazione nel settore pubblico (la versione consolidata è stata adottata dal legislatore europeo nel giugno 2013[327]) nonché (ii) finanziare la ricerca, lo sviluppo e l'innovazione in materia di dati aperti e (iii) sostenere le infrastrutture per i dati[328]. I suddetti interventi dimostrano appunto la centralità del tema in esame, soprattutto per le implicazioni economiche ad esso connesse.

[324] Ovvero la gestione di processi e comunicazioni della P.A. attraverso l'uso delle TIC.

[325] Nell'ambito del Piano d'azione rientra il documento "*G8 Open Data Charter*", siglato il 17 giugno 2013, nel quale sono stati statuiti i seguenti principi per l'implementazione di politiche ed azioni in materia di "*Open Data*": "*1: Open Data by Default, 2: Quality and Quantity, 3: Usable by All, 4: Releasing Data for Improved Governance, 5: Releasing Data for Innovation*".

[326] Per ogni ulteriore approfondimento sul programma comunitario si rinvia alla *homepage* consultabile all'indirizzo http://ec.europa.eu/programmes/horizon2020/.

[327] Le recenti modifiche alla direttiva citata incoraggiano gli Stati membri a mettere a disposizione i dati pubblici in formati aperti, allo scopo di garantire maggiore trasparenza nel settore pubblico e migliori condizioni per lo sviluppo economico.

[328] Tra cui ad esempio la creazione dell'"*Open Data Portal*", disponibile all'indirizzo https://open-data.europa.eu/en/data/.

4.1 LA RISPOSTA ITALIANA AL PROCESSO DI APERTURA DEI DATI

Alle proposte europee fanno eco quelle italiane[329], in cui l'apertura dei dati non soltanto rientra tra i pilastri dell'Agenda digitale italiana (nata per tradurre la strategia "Europa 2020" in obiettivi nazionali), ma ha trovato posto in disposizioni normative concrete (sebbene talora contraddittorie) a partire dall'anno 2010[330].

Per la diffusione degli "*Open Data*" nel contesto italiano è stata, tra gli altri, determinante l'iniziativa, avviata nel 2010 da "FORMEZ", "FORUM PA" e "Mobnotes.com", "MiaPA. La tua voce per migliorare la Pubblica Amministrazione", una piattaforma di *social check-in* per l'individuazione, la socializzazione e la valutazione di luoghi di interesse comune. Con "MiaPA" è stato realizzato un *database* in formato aperto, contenente tutti gli indirizzi della P.A., riutilizzabili da soggetti pubblici o privati per la realizzazione di nuovi servizi di pubblica utilità; tale iniziativa ha, inoltre, portato alla definizione e diffusione della licenza "*Italian Open Data License v1.0*" per la condivisione di dati pubblicati dalla P.A.

Parimenti rilevanti per la promozione di una cultura sull'apertura dei dati nonché per una sua effettiva realizzazione ad opera degli enti pubblici, sono state, da una parte, la pubblicazione del "Vademecum Open Data. Come rendere aperti i dati delle pubbliche amministrazioni" (v. Beta 2011), documento incentrato sul processo di apertura dei dati del settore pubblico, dall'altra, il *contest* "*Apps4Italy*", coordinato dal "Comitato Apps4Italy" e promosso dal "Dipartimento per la Digitalizzazione della PA e l'innovazione

[329] Interessante il "*Dossier Speciale Open Data 2010/2014, quattro anni di approfondimenti*", realizzato da Forum PA in occasione della "*International Open Data Day*" tenutasi il 22 febbraio 2014 e consultabile all'indirizzo http://saperi.forumpa.it/story/75211/dossier-speciale-open-data-20102014-quattro-anni-di-approfondimenti.

[330] *Cfr*. art. 21(rubricato "Trasparenza sulle retribuzioni dei dirigenti e sui tassi di assenza e di maggiore presenza del personale"), Legge 18 giugno 2009 n. 69, *Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonchè in materia di processo civile*, pubblicato in G.U. n. 140 del 19.06.2009; art. 11 ("Trasparenza"), d.lgs. 150/2009, *Attuazione della legge 4 marzo 2009, n. 15, in materia di ottimizzazione della produttività del lavoro pubblico e di efficienza e trasparenza delle pubbliche amministrazioni*, pubblicato in G.U. n. 254 del 31.10.2009; Delibera n. 105/2010 Civit, *Linee guida per la predisposizione del Programma triennale per la trasparenza e l'integrità (articolo 13, comma 6, lettera e, del decreto legislativo 27 ottobre 2009, n. 150)*; art. 52 comma 1-*bis* ("Accesso telematico ai dati e documenti delle pubbliche amministrazioni"), d.lgs. 7 marzo 2005 n. 82, Codice dell'amministrazione digitale, pubblicato in G.U. n.112 del 16.05.2005, così come modificato; art. 9 ("Dati di tipo aperto e inclusione digitale"), d.L. 18 ottobre 2012 n. 179 (Ulteriori misure urgenti per la crescita del Paese, pubblicato in G.U. n. 245 del 19.10.2012) che modifica l'art. 52 del Codice dell'Amministrazione Digitale; "Linee guida per i siti *web* delle PA - art. 4 della Direttiva n. 8/2009 del Ministro per la pubblica amministrazione e l'innovazione", 2011 (elaborate da un gruppo di lavoro composto da "DigitPA", "Dipartimento per la funzione pubblica", "Dipartimento per la digitalizzazione e l'innovazione tecnologica" e "FormezPA"; AGENZIA PER L'ITALIA DIGITALE, PRESIDENZA DEL CONSIGLIO DEI MINISTRI, "Linee guida per la stesura di convenzioni per la fruibilità di dati delle pubbliche amministrazioni - art. 58 comma 2 del CAD", giugno 2013, v. 2.0.

tecnologica" in collaborazione con "FORMEZ PA" e "FORUM PA", voluto con l'obiettivo di facilitare l'incontro sul tema degli "*Open Data*" tra gli *stakeholders* interessati.

Per quanto riguarda i progetti e le azioni in essere, lo stato dell'arte nazionale è in continuo divenire ed ha coinvolto sia realtà non istituzionali sia realtà istituzionali, nel rispetto di quelle precondizioni auspicate da Tim Berners-Lee, secondo cui "*it* [i.e. la politica degli OD] *has to start at the top, it ha sto start in the middle and it has to start at the bottom*". A titolo esemplificativo, tra le idee più significative "nate dal basso" rientrano "Stati Generali dell'Innovazione"[331], "Spaghetti Opendata"[332] e "Associazione Openpolis"[333]; con riferimento alla P.A., l'istituzione che per prima ha pubblicato i propri *datasets* è stata la Regione Piemonte[334], cui hanno fatto seguito numerosi enti territoriali (ad oggi, Comune di Bologna, Comune di Firenze, Comune di Milano, Comune di Roma, Comune di Torino, Provincia autonoma di Trento, Provincia di Roma, Regione Emilia Romagna, Regione Liguria, Regione Lombardia, Regione Piemonte, Regione Puglia, Regione Toscana, Regione Veneto) e nazionali (CNR, Camera dei Deputati, Funzione Pubblica, INAIL, INPS, Istat, Ministero della Salute, Ministero dello Sviluppo Economico, Ministero per la coesione territoriale[335], Senato della Repubblica). Analogamente a quanto già accaduto in altri Paesi del mondo (USA, UK, Australia, Canada, Norvegia etc.), nel portale "dati.gov.it – I dati aperti della P.A.", messo a disposizione dal Governo italiano, sono fruibili i cataloghi e le informazioni riguardanti il panorama nazionale.

Prima di concludere i cenni sullo scenario italiano, una breve nota merita di essere fatta sull'attività, ad oggi svolta, dal Ministero della Salute in materia di "*Open Data*", attività da cui emerge, peraltro, il segnale positivo che questo ente pubblico ha dato circa il processo di apertura dell'informazione pubblica sanitaria, rendendo fruibili agli utenti interessati alcuni *datasets* concernenti il proprio dominio[336].

A tal fine, nel 2011, la Direzione Generale del Sistema Informativo e Statistico Sanitario, ha realizzato il sito www.dati.salute.gov.it nel quale, per ogni *dataset* pubblicato, è

---

[331] Ulteriori informazioni sono disponibili all'indirizzo http://www.statigeneralinnovazione.it/online/.
[332] La *homepage* dell'iniziativa è consultabile all'indirizzo http://www.spaghettiopendata.org/.
[333] Per approfondimenti si rinvia all'indirizzo http://www.openpolis.it/.
[334] Il sito *web* è accessibile all'indirizzo http://www.dati.piemonte.it/.
[335] "OpenCoesione" è "il primo portale sull'attuazione degli investimenti programmati nel ciclo 2007-2013 da Regioni e amministrazioni centrali dello Stato con le risorse per la coesione" che consente ai cittadini di valutare l'efficacia delle risorse impiegate nonché la corrispondenza ai propri bisogni delle azioni intraprese. L'*homepage* del Progetto è disponibile all'indirizzo http://opencoesione.gov.it/.
[336] Attualmente, sono, ad esempio, disponibili *datasets* su farmacie, ASL, dispositivi medici, distributori di farmaci etc.

presente una scheda esplicativa sul "dato" ("licenza", "tipo di file", "*download*") e sulle "informazioni sul dato" ("descrizione", "*link* correlati", "argomenti", "formato di dati", "frequenza di aggiornamento", "data di caricamento", "data ultimo aggiornamento", "data ultima modifica metadato", "fonte", "pubblicato attraverso", "unità organizzativa", "nome funzionario", "*permalink*", "TAG"). Si segnala che, per quanto attualmente osservabile, la licenza utilizzata è la "*Italian Open Data Licence v2.0*"[337] ed i dati resi pubblici sono disponibili in un formato strutturato non proprietario quale "*Comma Separated Value*". Inoltre, rispondendo alle attese del legislatore italiano in merito alla "promozione della diffusione di architetture di *cloud computing* per le attività e i servizi delle pubbliche amministrazioni"[338], per la pubblicazione di dati aperti, il Ministero della Salute ha utilizzato un'infrastruttura di tipo "*Cloud*"[339].

Interessante, infine, formulare alcune considerazioni in merito alle modalità di ricerca dell'informazione all'interno di dati.salute.gov, che, di certo risponde ai criteri della navigazione "*user-friendly*". A partire dalla *homepage*, la navigazione può procede per: (a) parole libere ("che cosa stai cercando?"); (b) "ultimi dati catalogati"; (c) "TAG"; (d) "dati più scaricati"; (e) "*cloud*" ovvero (f) "ricerca avanzata" (*cfr. fig. 16*). In quest'ultimo caso, l'utente può scegliere tra i campi di ricerca selezionati: "argomento"[340], "tipo di dato"

[337] Le "condizioni della licenza" sono definite al paragrafo 2 che così dispone: "Il Licenziante concede una licenza per tutto il mondo, gratuita, perpetua, non revocabile e non esclusiva alle condizioni di seguito indicate: Sei libero di: - riprodurre, distribuire al pubblico, concedere in locazione, presentare e dimostrare in pubblico, comunicare al pubblico, messa a disposizione del pubblico inclusa, trasmettere e ritrasmettere in qualunque modo, eseguire, recitare, rappresentare, includere in opere collettive e/o composte pubblicare, estrarre e reimpiegare le Informazioni; - creare un Lavoro derivato ed esercitare sul Lavoro derivato i diritti di cui al punto precedente, per esempio attraverso la combinazione con altre informazioni (mashup). A condizione di: - indicare la fonte delle Informazioni e il nome del Licenziante, includendo, se possibile, una copia di questa licenza o un collegamento (link) ad essa; - non riutilizzare le Informazioni in un modo che suggerisca che abbiano carattere di ufficialità o che il Licenziante approvi l'uso che fai delle Informazioni; - prendere ogni misura ragionevole affinché gli usi innanzi consentiti non traggano in inganno altri soggetti e le Informazioni medesime non vengano travisate".

[338] Decreto-legge 9 febbraio 2012 n. 5, *Disposizioni urgenti in materia di semplificazione e di sviluppo*, pubblicato in G.U. n. 33 del 09.02.2012, convertito con modificazioni dalla legge 4 aprile 2012 n. 35.

[339] Come meglio in proposito precisato dal Ministero, "La soluzione sperimentata è basata sulla tecnologia *Cloud PaaS Platform as a Service* (*Microsoft Azure*) e del *toolkit*, gratuito e *Open Source*, denominato *OGDI – Open Government Data Initiative*: mediante tale soluzione sono resi disponibili in questo portale una serie di strumenti *cloud-based* aperti e interoperabili per lo sviluppo rapido ed economico di servizi a valore aggiunto per cittadini/aziende/altre PA senza alcun vincolo di realizzazione (sono possibili linguaggi .NET, PHP, Ruby, Python ecc.)". Per ulteriori indicazioni si rinvia alla pagina dedicata http://opendatasalute.cloudapp.net/.

[340] Quelli presenti sono: Alimenti, Assistenza ospedaliera, Assistenza territoriale, Benefici, Comunicazione, Cure, Dispositivi medici, Elenco Nazionale Direttori, Farmaci, Innovazione, Medicinali Veterinari, Nutrizione, Prevenzione, Professioni, Programmazione, Ricerca, Risorse umane, Sistema informativo, Statistiche del SSN, Territorio e popolazione, Tracciabilità del Farmaco, Veterinaria, Vigilanza.

(alfanumerico, dato geografico), "tipo di file" (XLS, ODS, XML, CSV, SHP, HTML), "periodo di riferimento" (2013, 2012, 2011, 2010), "TAG"[341].

Iniziando la propria navigazione dalla *homepage*, l'utente può, altresì, accedere direttamente alla sezione "Dati", nella quale sono consultabili i *dataset* pubblicati (ed in costante aggiornamento), scegliendo le modalità di visualizzazione attraverso l'operazione "ordina per" ("ultimo aggiornamento *dataset*", "ultima modifica metadato", "voti ricevuti", "ordine alfabetico", "tipo di dato".

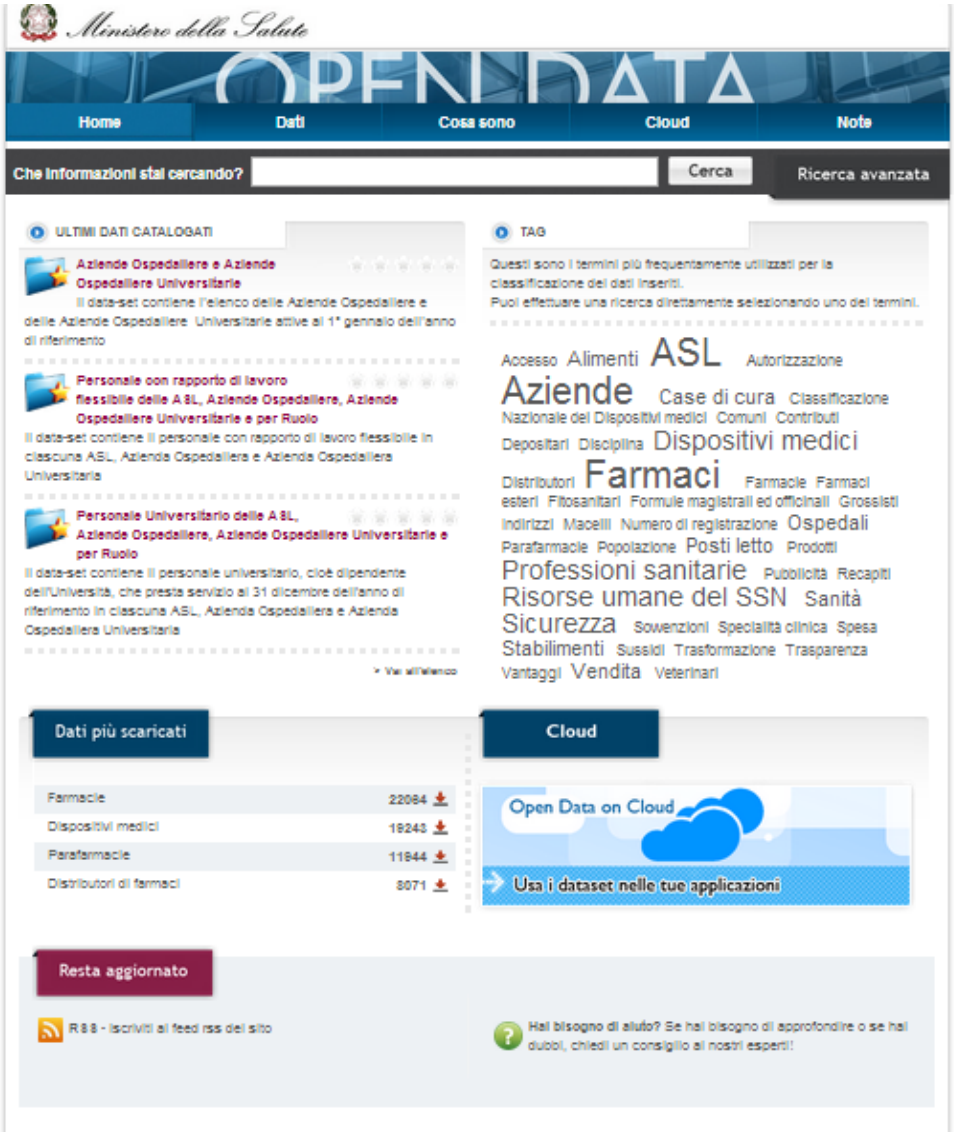


Figura 16 - *Screenshot* www.dati.salute.gov (ultimo accesso: maggio 2014)

[341] Ad oggi: Accesso - Alimenti - ASL - Autorizzazione - Aziende - Case di cura - Classificazione Nazionale dei Dispositivi medici - Comuni - Contributi - Depositari -Disciplina - Dispositivi medici - Distributori - Farmaci - Farmacie - Farmaci esteri - Fitosanitari - Formule magistrali ed officinali - Grossisti -Indirizzi - Macelli - Numero di registrazione - Ospedali - Parafarmacie - Popolazione - Posti letto - Prodotti - Professioni sanitarie - Pubblicità -Recapiti - Risorse umane del SSN - Sanità - Sicurezza - Sovvenzioni - Specialità clinica - Spesa - Stabilimenti - Sussidi - Trasformazione - Trasparenza - Vantaggi - Vendita - Veterinari.

4.2 GLI "*OPEN DATA*" ED I "*LINKED OPEN DATA*" COME STRUMENTO DI INTEROPERABILITÀ

L'importanza politico-economica che il fenomeno "*Open Data*" assume è dovuta proprio al nuovo paradigma adottato per la gestione dei dati pubblici: l'accessibilità.

"*A piece of content or data is **open** if anyone is free to use, reuse, and redistribute it – subject only, at most, to the requirement to attribute and share-alike*"[342].

(i) Disponibilità ed accessibilità dei dati a costi non superiori a quelli di riproduzione, in tempi celeri e con un livello di granularità elevato, (ii) riuso e redistribuzione dell'informazione, combinabile con quella contenuta in altri *dataset*, (iii) partecipazione universale, garantita attraverso l'adozione di licenze "aperte" che concedano all'utente la possibilità di riprodurre, distribuire, trasmettere ed adattare liberamente i dati, anche a scopi commerciali, citandone la fonte, sono, dunque, le peculiarità di dati che si intendono "aperti".

Affinché il risultato desiderato, in termini di apertura e, dunque, di fruibilità, sia possibile, è indispensabile seguire dei criteri precisi, corrispondenti a quelli indicati in *figura 17*[343].

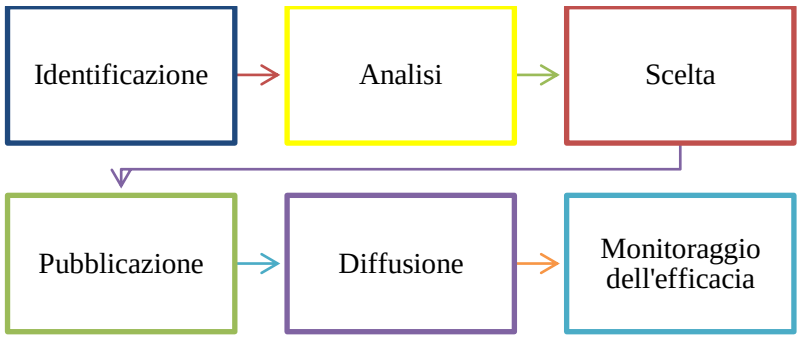


Figura 17 - Step per il processo di apertura dei dati

[342] OPEN DEFINITION, *Defining the Open in Open Data, Open Content and Open Services*, 2012.

[343] Esula dal presente lavoro soffermarsi sulle modalità operative attraverso cui realizzare il processo di apertura dei dati. Diversi sono i prototipi e le *best practices* che si stanno affermando tanto a livello internazionale quanto a livello nazionale e regionale. Una valida guida operativa è senz'altro costituita da OPEN KNOWLEDGE FOUNDATION, *Open Data Handbook Documentation - Release 1.0.0*, November 14, 2012, pp. 23. In particolare, nel paragrafo dedicato alle modalità di apertura dei dati, si trovano le seguenti indicazioni: "*There are four main steps in making data open, each of which will be covered in detail below. These are in very approximate order - many of the steps can be done simultaneously. 1. Choose your dataset(s). Choose the dataset(s) you plan to make open. Keep in mind that you can (and may need to) return to this step if you encounter problems at a later stage. 2. Apply an open license. (a) Determine what intellectual property rights exist in the data. (b) Apply a suitable 'open' license that licenses all of these rights and supports the definition of openness discussed in the section above on 'What Open Data' (c) NB: if you can't do this go back to step 1 and try a different dataset. 3. Make the data available - in bulk and in a useful format. You may also wish to consider alternative ways of making it available such as via an API. 4. Make it discoverable - post on the web and perhaps organize a central catalog to list your open datasets.*".

Nel processo di selezione dei *dataset* occorre, in particolare, tenere presente, da una parte, le scelte strategiche e politiche in essere nonché gli orientamenti della cittadinanza, dall'altra, i risultati di un'attenta ed adeguata analisi giuridica che, attenzionata la natura del dato, ne escluda l'inutilizzabilità nei casi, ad esempio, di dati sensibili o oggetto di diritto d'autore o segreto industriale. Il tema in esame involge, inoltre, questioni di diritto che impegnano la dottrina, tra cui, la definizione delle *policy* di licenza d'uso, il diritto all'oblio, il rapporto tra de-anonimizzazione e re-identificazione etc.

La distribuzione delle informazioni non esaurisce, però, il compito degli enti pubblici: se, per gli utenti, infatti, è importante conoscere quali dati siano disponibili, per essi è maggiormente rilevante sapere che quegli stessi dati siano riutilizzabili, e cioè, che attraverso le informazioni rese pubbliche sia possibile produrre nuova conoscenza e nuovo valore. Quest'idea introduce il concetto di "grado di apertura" dei dati, di cui una paradigmatica classificazione è stata fornita da Tim Berners-Lee. Tale classificazione si basa su cinque livelli progressivi, a ciascuno dei quali è stato assegnato un numero di stelle corrispondente al singolo livello (c.d. "*5-star rating scheme*"); in particolare:

- 1 stella, se il dato è disponibile sul *web*, in qualsiasi formato ma con una licenza aperta;
- 2 stelle, se il dato è disponibile in un formato strutturato che può essere interpretato da un *software* (e.g. *Microsoft Excel*);
- 3 stelle, se il dato è in un formato strutturato non proprietario (e.g.: *Comma Separated Value*[344]);
- 4 stelle, se, oltre a rispettare tutti i criteri precedenti, il dato fa uso di *standard* per identificare i dati, affinché le applicazioni possano utilizzarli per comprenderne il contenuto informativo;
- 5 stelle, se il dato rispetta tutti gli altri criteri e contiene collegamenti ad altri dati al fine di fornire un contesto alle proprie informazioni (*Linked Open Data*) [345].

L'implicazione più significativa del processo di apertura dell'informazione è la capacità di inter-operare, ossia di scambiare informazioni in modo automatico, di *dataset* provenienti da sistemi ed organizzazioni diversi. La possibilità di ottenere sistemi informativi di fatto interoperabili assume una rilevanza non trascurabile sia nella prospettiva pubblica sia in quella privata; in un certo senso è, infatti, possibile affermare

[344] Formato di file di testo che consente di rappresentare dati alfanumerici di una tabella.
[345] T. BERNERS-LEE, *Is your Linked Open Data 5 Star?*, 2009.

che l'interoperabilità, realizzabile anche grazie all'apertura dei dati, rappresenta la chiave per lo sviluppo di prodotti e servizi.

Lo scenario illustrato rivela ancora una volta la complessità culturale, legislativa e tecnologica che involge il suddetto processo. Affinché l'interoperabilità sia efficacemente raggiunta, è, però, essenziale che siano egualmente promossi tanto i profili tecnici (di cui è parte il confronto e l'integrazione dell'informazione *tout court*) quanto quelli semantici ed organizzativi[346]. Infatti, lo scambio dei dati, la definizione di *policy* sull'utilizzo dell'informazione e sulla protezione dei dati personali, la condivisione di modelli di *business* e delle regole sulle licenze d'uso rappresentano solo una esemplificazione del principio di interoperabilità già esaminato.

Congiuntamente alle azioni politico-normative comunitarie e nazionali fin qui ricordate, è, dunque, indispensabile che la Pubblica Amministrazione si orienti verso il modello "*Linked Open Data*", definito da Tim Berners-Lee nel 2006 e la cui peculiarità va ravvisata nell'attenzione all'interoperabilità semantica dei dati, raggiunta attraverso l'"identità" assegnata all'informazione, per mezzo degli strumenti già definiti ed implementati nel *Semantic Web*. Tra questi, l'utilizzo di: (i) *Uniform Resource Identifier* (URI) come identificativo di ciò che è referenziato sul *web*; (ii) protocollo HTTP (*Hypertext Transfer Protocol*) per la comunicazione e lo scambio dei dati; (iii) RDF (*Resource Description Framework*) come modello per rappresentare le relazioni tra le informazioni[347]; (iv) SPARQL (*SPARQL Protocol and RDF Query Language*) come linguaggio di interrogazione dei dati rappresentati in RDF; (v) *link* ad altre entità o concetti identificati con URI e reperibili sul *Web*[348]. I collegamenti diretti tra dati identici o in relazione, appartenenti a sorgenti (*database*) diverse, facilitano il riuso automatico dell'informazione da parte di soggetti terzi mediante l'utilizzo di *software*; come già ricordato, tale effetto è, di estremo valore sociale ed economico, giacché consente la realizzazione e la diffusione di nuovi servizi.

---

[346] Sul concetto di interoperabilità nel senso ivi espresso, si rinvia a: EUROPEAN COMMISSION, *European Interoperability Framework for Pan-European egovernment Services*, Luxemburg, 2004, pp.26; EUROPEAN COMMISSION, *Annex 2 to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions "Towards interoperability for European public services"*, COM(2010) 744 final.

[347] RDF permette di rappresentare dati e metadati attraverso la definizione di asserzioni (*statements*), dette triple, secondo lo schema <soggetto> <proprietà> <oggetto>.

[348] Le indicazioni fornite nel 2006 da Tim Berners-Lee in merito alle modalità di pubblicazione dei dati nel *web* sono accessibili all'indirizzo http://www.w3.org/DesignIssues/LinkedData.html. Per ulteriori approfondimenti si rinvia a: T. HEATH, C. BIZER, *Linked Data: Evolving the Web into a Global Data Space* (1st edition), Synthesis Lectures on the Semantic Web: Theory and Technology, 1:1, 1-136, Morgan & Claypool, 2012.

Lo stato dell'arte su *LOD* rivela un panorama internazionale e nazionale certamente eterogeneo, nel quale sono, però, presenti valide iniziative (strategie politiche, disposizioni normative, studi, progetti, *best practice* etc.) per l'adozione ed implementazione delle tecnologie utili alla creazione di "*Linked Open Data*"[349]. Esemplificativo il progetto W3C "*Linking Open Data*"[350], grazie al quale è in costante crescita il numero di *dataset* pubblicati sul *web* in RDF, così come sono in aumento i "RDF *link*" tra i dati provenienti da risorse diverse. Sulla piattaforma "*Datahub*"[351], voluta da *Open Knowledge Foundation*, è possibile cercare i dati di interesse, registrare *datasets* pubblicati nonché creare e gestire gruppi di *dataset*.

5. IL FASCICOLO SANITARIO ELETTRONICO COME FONTE DI CONOSCENZA SCIENTIFICA

L'opportunità di "aprire" i dati de-identificati raccolti in archivi diversi da quelli socio-sanitari, tra cui, ad esempio, i FSE, è al centro delle riflessioni del presente capitolo (*cfr. fig. 14*)[352]. Significativo in proposito ricordare che l'imperativo "*Liberate the data*" coincide, tra l'altro, con il secondo livello di cambiamento individuato dalla *eHealth Task Force* nel rapporto "*Redesigning health in Europe for 2020*"[353]. Tuttavia, secondo quanto asserito dagli esperti della *Task Force*, affinché un reale cambiamento verso l'"apertura" sia possibile, è urgente: (i) sul fronte legislativo, definire *standard* per il trattamento dei dati e per garantire un trattamento uniforme dell'informazione tra i 27 Paesi membri; (ii) costituire un gruppo di lavoro europeo che individui *best practice* e *e-Health model* in materia di "*Open Data*"; (iii) promuovere, tra consumatori e specialisti, una cultura sull'utilizzo di *e-Data* de-identificati per usi secondari[354].

Le raccomandazioni summenzionate hanno come principale obiettivo l'accelerazione del processo di innovazione nel settore sanitario, anche grazie alla diffusione, a costi

[349] Su questo punto vedasi: COMMISSIONE DI COORDINAMENTO SPC (Sistema Pubblico di Connettività e Cooperazione), *Linee guida per l'interoperabilità semantica attraverso i Linked Open Data*, v. 1.3, 30 luglio 2012, pp. 102.

[350] W3C, *Linking Open Data*, 2012.

[351] Consultabile all'indirizzo http://datahub.io.

[352] Interessante l'esperienza condotta presso la Mayo Clinic in merito all'applicazione dei principi LOD alle informazioni sanitarie contenute nei FSE; lo studio è presentato in J. PATHAK, R. C. KIEFER, C. G. CHUTE, *Applying linked data principles to represent patient's electronic health records at Mayo clinic: a case report*, Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium, ACM New York, USA, 2012, pp. 455-464.

[353] Del citato rapporto si è già parlato nel capitolo I del presente lavoro al quale, pertanto, si rinvia.

[354] Per approfondimenti: H.C. KUM, S. AHALT, *Privacy-by-Design: Understanding Data Access Models for Secondary Data*, AMIA Summits Transl Sci Proc., 2013 Mar 18; 2013:126-30; B. MALIN, D. KARP, R.H. SCHEUERMANN, *Technical and policy approaches to balancing patient privacy and data sharing in clinical and translational research*, J Investig Med., 2010 Jan; 58(1):11-8.

ragionevolmente contenuti, di dati sanitari utilizzabili per finalità di ricerca; fondamentali, in questo senso, i requisiti di "qualità" e granularità che l'informazione sanitaria digitale deve possedere.

Come ricordato da Neelie Kroes, Vicepresidente e Commissario europeo per l'Agenda digitale per l'Europa, diversi progetti, finanziati dall'UE, stanno contribuendo al raggiungimento dei summenzionati scopi attraverso la creazione di un idoneo substrato tecnologico[355]; con riferimento al Fascicolo Sanitario Elettronico – ha precisato Kroes – si possono ad esempio ricordare: (i) "*the SemanticHealthNet*", finalizzato all'interoperabilità semantica di conoscenza clinica e biomedica[356]; (ii) "*the EU ADR*"[357], volto a sviluppare un sistema informatizzato di rilevazione delle reazioni avverse provocate da farmaci, integrato da sistemi di segnalazione spontanea (di interesse evidenziare che, per raggiungere l'obiettivo, il Progetto utilizza dati clinici provenienti da oltre 30 milioni di EHR di selezionati paesi europei, tra cui Paesi Bassi, Danimarca, Regno Unito e Italia); (iii) "*the TRANSFoRm*"[358], basato su riutilizzo dell'informazione clinica contenuta nel FSE per finalità di cure primarie; (iv) "*the TAS3*"[359], nato con l'obiettivo di sviluppare un'architettura IT per la gestione ed elaborazione di informazioni personali distribuite.

Parimenti importante, per le finalità summenzionate, è il progetto triennale "*Linked2Safety*" (1 ottobre 2011 - 30 settembre 2014). Attività e scopi del "*Consortium*" istituito per realizzarlo, sono efficacemente sintetizzate dalle parole chiave che titolano il Progetto: "*A Next-Generation, Secure Linked Data Medical Information Space For Semantically-Interconnecting Electronic Health Records and Clinical Trials Systems Advancing Patients Safety In Clinical Research*"; per ciò che attiene il presente studio è essenziale evidenziare l'interesse verso l'utilizzo di informazioni contenute nei FSE dei pazienti per gli usi di professionisti sanitari, ricercatori clinici e aziende farmaceutiche, nel pieno rispetto delle normative comunitaria e nazionali in materia di protezione dei dati personali. I risultati auspicati sono così sintetizzati: "*With the developed reference*

---

[355] Interessante su questo aspetto il seguente rapporto: EUROPEAN COMMISSION, *Unlocking the ICT growth potential in Europe: Enabling people and businesses*, Luxemburg, 2014, che, nel sottolineare l'importanza che l'ICT sta assumendo nel settore sanitario, evidenzia la necessità di dar vita a progetti europei effettivamente implementabili, nei quali, pertanto, devono essere tenuti presenti i profili dell'interoperabilità dei sistemi, dell'utilizzo di *standards* e della tutela dei dati personali. Per approfondimenti sulle tematiche giuridiche, vedasi: H. SUOMINEN, *Towards an international electronic repository and virtual laboratory of open data and open-source software for telehealth research: comparison of international, Australian and Finnish privacy policies*, Stud Health Technol Inform., 2012; 182:153-60.

[356] La *homepage* è consultabile all'indirizzo http://www.semantichealthnet.eu/.

[357] La *homepage* è consultabile all'indirizzo http://www.euadr-project.org/.

[358] La *homepage* de "*Translational Research and Patient Safety in Europe*" *project* è consultabile all'indirizzo http://www.transformproject.eu/.

[359] "*Trusted Architecture for Securely Shared Services*".

architecture, data protection framework, common EHR schema, lightweight semantic model and integrated platform will facilitate the scalable and standardized semantic interlinking, sharing and reuse of heterogeneous EHR repositories"[360].

Analogamente a quanto osservato nei capitoli precedenti, gli esempi riportati dimostrano che la velocità con cui tecnologia, evidenza clinica e diritto procedono è difforme: se, da una parte, attraverso la realizzazione ed implementazione dei progetti comunitari si propone di dar vita a strumenti all'avanguardia rispetto ai nuovi scenari, al contempo, rappresenta un enorme ostacolo all'apertura dei dati sanitari la questione della *privacy*, di cui sono, tra gli altri, una palese realtà, la scarsità di *case-study* e di documenti metodologici che, viceversa, potrebbero contribuire ad un dialogo sistematico che riguardi il settore sanitario.

In riferimento agli aspetti di diritto, rimangono certamente validi i principi già affermati dalla direttiva comunitaria e dalla legislazione nazionale vigente in materia di trattamento dei dati personali e sensibili, quali: (i) il rilascio di adeguata informativa al paziente sulla pertinenza e non eccedenza dei dati rispetto alle finalità di trattamento; (ii) l'ottenimento del consenso informato dei pazienti da parte dei responsabili del trattamento[361]; (iii) la tutela dei diritti dell'assistito (ad esempio, il diritto all'oblio); (iv) la responsabilità a carico delle figure autorizzate *ex lege* al trattamento dei dati.

La possibilità di applicare i principi degli "*Open Data*" e "*Linked Open Data*" al FSE concerne, dunque, esclusivamente (non potrebbe essere diversamente, non soltanto per ragioni giuridiche ma anche per motivi etici) informazioni sanitarie de-identificate, cioè, dati criptati che escludano, dunque, di risalire all'identità del singolo paziente.

Nonostante le criticità, giuridiche e tecnologiche, sottese a tale tesi, per tutti i motivi fin'ora illustrati e tenuta presente un'analisi costi-benefici, è opportuno valutarne la fattibilità, a beneficio della salute tanto individuale quanto collettiva.

Delle novità legislative introdotte nell'ordinamento giuridico italiano si è già dato conto nei capitoli precedenti; in questa sede si richiama il contenuto di alcune disposizioni di cui al decreto-legge 179/2012[362], in particolare, il comma 2, lettere b) e c), dell'articolo 12, in cui è rispettivamente stabilito che il FSE è istituito, oltre che per motivi di prevenzione, diagnosi e cura, anche per usi secondari e di salute pubblica, nonché il comma 6, dello stesso articolo che così recita: "Le finalità di cui alle lettere b) e c) del comma 2 sono

[360] La *homepage* del Progetto è consultabile all'indirizzo http://www.linked2safety-project.eu/.
[361] *Ex* artt. 106, 107 e 110 del Codice *privacy*.
[362] Convertito, con modificazioni, dalla legge 22/2012.

perseguite senza l'utilizzo dei dati identificativi degli assistiti presenti nel FSE, secondo livelli di accesso, modalità e logiche di organizzazione ed elaborazione dei dati definiti con decreto, in conformità ai principi di proporzionalità, necessità e indispensabilità nel trattamento dei dati personali". La volontà del legislatore italiano sembra, dunque, andare nella direzione di un generale beneplacito verso l'utilizzo dei FSE meglio, dei dati de-identificati in essi contenuti, come fonti di informazione per finalità di ricerca.

Altrettanto rilevante richiamare il recente provvedimento dall'autorità italiana Garante per la protezione dei dati personali in tema di "trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale": "[…]1.2. L'autorizzazione è rilasciata, altresì, ai seguenti soggetti: a) alle persone fisiche o giuridiche, agli enti, alle associazioni e agli altri organismi privati, per scopi di ricerca scientifica, anche statistica, finalizzata alla tutela della salute dell'interessato, di terzi o della collettività in campo medico, biomedico o epidemiologico, allorché si debba intraprendere uno studio delle relazioni tra i fattori di rischio e la salute umana anche con riguardo a studi nell'ambito della sperimentazione clinica di farmaci, o indagini su interventi sanitari di tipo diagnostico, terapeutico o preventivo, ovvero sull'utilizzazione di strutture socio-sanitarie, e la disponibilità di dati solo anonimi su campioni della popolazione non permetta alla ricerca di raggiungere i suoi scopi. *In tali casi, il trattamento può comprendere anche dati idonei a rivelare la vita sessuale e l'origine razziale ed etnica solo ove indispensabili per il raggiungimento delle finalità della ricerca. Inoltre, occorre acquisire il consenso (in conformità a quanto previsto dagli artt. 106, 107 e 110 del Codice), e il trattamento successivo alla raccolta non deve permettere di identificare gli interessati anche indirettamente, salvo che l'abbinamento al materiale di ricerca dei dati identificativi dell'interessato sia temporaneo ed essenziale per il risultato della ricerca, e sia motivato, altresì, per iscritto. I risultati della ricerca non possono essere diffusi se non in forma anonima.* Resta fermo quanto previsto dall'art. 98 del Codice"[363]. Tali affermazioni hanno una portata rilevante, in linea con le recenti modifiche legislative di cui sopra: se, da una parte sottolineano il primato del diritto alla *privacy*, dall'altra riconoscono e riaffermano l'utilità dei dati sanitari per finalità secondarie, seppur nel caso di specie trattasi di informazioni sensibili e non di informazioni de-identificate.

[363] *Cfr.* GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Autorizzazione n. 2/2013 - Autorizzazione al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale*, pubblicata in G.U. n. 302 del 27.12.2013, valida dal 1° gennaio 2014 al 31 dicembre 2014, salve eventuali modifiche del Garante.

Un effetto positivo immediato dell'utilizzo dei dati sanitari raccolti nel FSE potrebbe, tra gli altri, riscontrarsi nell'implementazione dei "registri per patologia", ovvero quei sistemi centralizzati contenenti dati relativi a precise malattie, essenziali per le ricerche in campo epidemiologico, clinico-sperimentale, di prevenzione sanitaria etc. [364] e condivisi a livello comunitario, come nel caso del progetto europeo "EPIRARE", per la creazione di una piattaforma europea per la registrazione di dati sulle persone affette da malattie rare[365].

Il Fascicolo Sanitario Elettronico è uno strumento preziosissimo dal punto di vista della quantità di dati sulla salute; ciò è particolarmente vero se si esamina il contesto europeo ed internazionale, verso il quale la mobilità transfrontaliera orienta[366]. Il numero di informazioni raccolte è elevato ed un livello di granularità eccellente potrebbe aprire a nuovi scenari per la ricerca e la salute pubblica. Paradigmatici esempi che tentano, in modo il più possibile uniforme, di sintetizzare i profili tecnologico, giuridico e sanitario, sono, tra gli altri, (i) lo studio condotto da El Eman (*et alii*) con il quale i ricercatori hanno dimostrato la fattibilità dell'apertura dei dati sanitari, con rischi trascurabili ("*acceptably low*") di re-identificazione, in contesti mondiali di *datasets* longitudinali [367] nonché (ii) l'attività portata avanti da "*The Centre for Health Record Linkage*" (CHeReL), nato nel 2006 in Australia e diretto dal Ministero della Salute, allo scopo di aiutare ricercatori e *policy makers* nell'accesso ai *linked data* sanitari del Paese, seguendo un sistema forte di de-identificazione e, dunque, di protezione dei dati sensibili[368].

Ripensare all'architettura e, dunque, al *design* del FSE, tenendo presenti la "*Privacy by Design*" e gli "*Open Data*", è una via ipotizzabile, capace di coniugare i diritti del paziente con il valore economico della conoscenza. A tal fine è auspicabile che prosegua il dialogo tra studiosi e *pratictioner* nonché tra esperti afferenti alle varie discipline coinvolte affinché sia rispettata e messa in atto una progettazione *by default* del FSE contemperante tutti gli interessi coinvolti.

---

[364] Interessante il recente parere del GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Trattamento di dati personali contenuti nel Registro Italiano di Dialisi e Trapianto - 16 gennaio 2014*, Registro dei provvedimenti n. 16 del 16 gennaio 2014, con il quale l'Autorità ha vietato agli enti privati che si occupano di ricerca medico-epidemiologica l'utilizzo di dati personali raccolti dalle strutture pubbliche di dialisi in assenza di informativa ai pazienti in cura e relativo rilascio consenso. In alternativa - ha chiarito il Garante - devono essere utilizzati esclusivamente dati anonimi.

[365] Nato nell'aprile 2011, il progetto triennale è finanziato dalla Direzione Sanitaria e dei Consumatori della Commissione Europea (DG-SANCO) ed è coordinato dall'Istituto Superiore di Sanità. La *homepage* è consultabile all'indirizzo http://www.epirare.eu/.

[366] Vedasi la già citata *Directive 2011/24/EU on the application of patients' rights in cross-border healthcare*, recepita dall'Italia il 28 febbraio 2014, con l'approvazione del decreto legislativo di recepimento approvato dal Consiglio dei Ministri.

[367] *Cfr.* K. EL EMAM et al., *De-identification methods for open health data: the case of the Heritage Health Prize claims dataset*, J Med Internet Res., 2012, Feb 27; 14(1):e33.

[368] Il sito del CHeReL è accessibile all'indirizzo http://www.cherel.org.au/.

Se, da una parte, infatti, di per sé l'accesso al FSE è esclusivo del personale sanitario autorizzato (medico e para-medico), dotato dei già ricordati strumenti identificativi necessari per motivi giuridici e di sicurezza, al contempo, non è impossibile immaginare la definizione di regole che separino, in modo certo, i dati sensibili dalle informazioni clinico-sanitarie (riferite, ad esempio, a immagini, esiti di laboratorio, parametri significativi per patologia). È proprio su questi dati che potrebbe ipotizzarsi una modellazione in linea con i principi dei "*Linked Open Data*".

Nel FSE un ruolo centrale è attribuibile al Codice Fiscale, identificativo univoco del cittadino/paziente. Gli attuali sistemi permettono di cifrare questo dato ed estrarre conoscenza aggregata per motivi di sanità pubblica (ad esempio, da parte degli uffici territoriali al fine di monitorare la spesa farmaceutica distrettuale). Tuttavia, in questo caso, l'identificazione del singolo è possibile; questo elemento costituisce una forte criticità nell'ipotesi di apertura di dati che siano, quindi, conoscibili anche da soggetti non dedicati alla cura del paziente. De-identificare, di fatto, le informazioni collezionate nei FSE è, dunque, presupposto per la realizzazione della tesi esposta (*cfr. fig.18*).

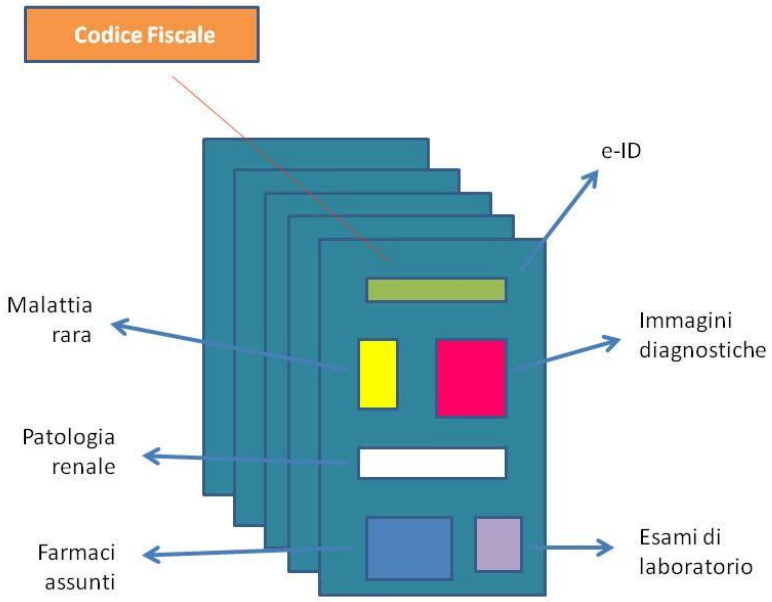


Figura 18 - I tipi di informazioni del FSE

CONCLUSIONI

All'esito del presente studio è difficile parlare di conclusioni; i profili esaminati, infatti, consentono di formulare rilevanti considerazioni che, parimenti evidenziano come la ricerca sia un *work in progress*[369].

Le ragioni di questa affermazione vanno, anzitutto, rintracciate nel fatto che sia le nuove tecnologie sia il diritto stanno vivendo un intenso processo di cambiamento ed il rapporto tra le due discipline non sempre è armonico. Giova, in proposito, richiamare il dilemma di Collingridge, secondo cui: "*Regulators having to regulate emerging technologies face a double-bind problem: the effects of new technology cannot be easily predicted until the technology is extensively deployed. Yet once deployed they become entrenched and are then difficult to change*"[370]. Tale asserzione aiuta ad inquadrare le problematiche fin qui illustrate e, in particolare, la complessità relazionale tra legislatori, giuristi, studiosi di etica e di bioetica, operatori sanitari, informatici e pazienti, soprattutto ai fini di una traduzione normativa in materia di sanità digitale e Fascicolo Sanitario Elettronico.

In un certo senso, analoghe difficoltà sono visibili sul fronte tecnologico: nella fase di progettazione dell'architettura di sistemi informativi sanitari, infatti, spesso prevale un approccio "tecno-centrico", in cui questioni giuridiche ed esigenze degli *user* (pazienti e/o operatori sanitari) sono frequentemente considerate non prioritarie.

Una prima considerazione, dunque. Sebbene la predisposizione di tavoli tecnici e di incontri fra esperti, a tutt'oggi sono riscontrabili ostacoli legati alla carenza operativa sul fronte dell'interdisciplinarietà. Ad esempio è possibile evidenziare che nella definizione degli atti legislativi manchi talora un approccio inclusivo delle nuove tecnologie, se non di tipo formale, di natura sostanziale. Inoltre, la dottrina giuridica, spesso, interpreta le fattispecie di sanità digitale, concernenti le presunte violazioni in materia di dati personali, secondo vecchi paradigmi, talora non abbastanza allineati con le effettive potenzialità dei nuovi strumenti.

Le previsioni di rango primario, recentemente introdotte nell'ordinamento giuridico italiano, se, da una parte, sono da apprezzare in quanto rispondono ad una necessità

[369] Non da ultimo, all'atto di redazione delle presenti conclusioni, è stato pubblicato il documento "*Linee guida per la presentazione dei piani di progetto regionali per il FSE*" del 31 marzo 2014, risultato del Tavolo tecnico istituito con Determinazione Commissariale n.184/2013 DIG del 21 novembre 2013, coordinato dall'Agenzia per l'Italia Digitale e dal Ministero della salute, con rappresentanti del Ministero dell'economia e delle finanze, delle Regioni e Province Autonome, nonché del Consiglio Nazionale delle Ricerche e del CISIS (Centro Interregionale per i Sistemi Informatici, Geografici e Statistici).

[370] *Cfr*. D. COLLINGRIDGE, *The Social Control of Technology*, St. Martin's Press, Frances Pinter, 1980.

emergente di cogenza normativa in tema di FSE, dall'altra non costituiscono un *corpus iuris* autonomo: la regolamentazione degli aspetti tecnici è affidata ad atti di futura emanazione (il primo è lo schema di decreto sul Fascicolo Sanitario Elettronico attualmente all'esame della Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e Bolzano di cui si è riferito nel presente lavoro) e, per quanto concerne il tema della protezione dei dati personali, la legge opera di fatto un mero rinvio al "Codice *privacy*".

Lungi dall'invocare previsioni normative che violino i diritti fondamentali dell'uomo, si ritiene, però, necessario tornare a riflettere sulle questioni astratte di sanità elettronica alla luce dei nuovi paradigmi giuridici, quali la "*Privacy by Design*". Le regole sulla *privacy* devono, in quest'ottica, diventare un'impostazione di *default* ed essere integrate nel *design* delle infrastrutture tecnologiche, affinché i dati dell'utente siano salvaguardati a priori dai sistemi stessi. Seppur possa apparire quadro puramente teorico ed ideale, è fortemente auspicabile un maggiore dialogo sostanziale per la definizione ed il coordinamento di norme, prassi e *policy*.

Questa prospettiva assume una particolare rilevanza nel contesto sanitario europeo, in cui l'assistenza sanitaria transfrontaliera è una realtà concreta, per di più regolata dalla direttiva 2011/24/UE, recepita dall'Italia con decreto legislativo approvato dal Consiglio dei Ministri il 28 febbraio 2014.

La mobilità dei cittadini europei urge sistemi informativi sanitari interoperabili, la definizione di una legislazione univoca tra i 27 Paesi membri in tema di protezione dei dati personali nonché *policy* aziendali chiare, in cui i principi di *security* e *privacy* siano armonicamente regolati.

Una seconda criticità emersa dall'analisi dello stato dell'arte va rintracciata nell'assenza di "clusterizzazione" delle esperienze nazionali in essere in tema di sanità digitale e di FSE.

Nel contesto comunitario è continuo il monito delle Istituzioni "a fare sistema" tra buone prassi ed azioni efficaci in essere tra i 27 Paesi membri.

Nonostante gli sforzi del Governo italiano per coordinare la capillare digitalizzazione sul fronte sanitario, sono ancora parecchie le difformità riscontrabili a livello territoriale e locale. I motivi sono da attribuire talora a deficit economici e ad inefficienze organizzative di talune realtà, tal'altra a fattori individuali degli *user*. Ad esempio, la ritrosia nell'utilizzo del FSE, e, prima, nel consenso all'attivazione del FSE, ha molteplici cause, molte delle

quali sono di tipo culturale, perlopiù legate al *digital divide*, qui inteso come mancanza di un'educazione all'utilizzo del digitale per l'accesso ai servizi sanitari.

Inoltre, nella prassi si registra una carente sensibilizzazione ed una diffusa sfiducia negli strumenti di e-*Health* tra cittadini ed operatori sanitari. A ciò si aggiunge una forte diffidenza nei confronti del sistema giuridico: i profili della responsabilità professionale e del trattamento dei dati sono solo due significativi esempi che fungono da deterrente nell'utilizzo di prodotti e servizi di sanità digitale.

Analogamente, sul fronte tecnologico talora manca, soprattutto a livello locale, una visione di lungo periodo: talune istituzioni sanitarie prediligono soluzioni tecniche provvisorie, idonee ad ottemperare solo formalmente alle istanze del legislatore.

Sebbene si sia consapevoli dei costi di un'iniziativa capillare di controllo e verifica dei sistemi informativi in essere, si è parimenti convinti della necessità e valenza di una simile azione, volta non soltanto ad individuare i problemi reali, ma, soprattutto, a formulare proposte operative concrete.

La suddetta scarsa lungimiranza tecnica degli enti sanitari locali italiani[371], è, ad esempio, rintracciabile nella strutturazione (o assenza di strutturazione) semantica dei dati sanitari, profilo, peraltro, alla base dell'interoperabilità delle informazioni collezionate dai sistemi informativi nonché centrale per un corretto processo di de-identificazione delle informazioni, anche per usi seondari di ricerca e salute pubblica.

Come emerso dal capitolo II, in tutti i progetti esaminati esiste un forte interesse nei confronti dell'infrastruttura tecnologica per il trasferirmento dei dati, sia in ambito nazionale sia in ambito comunitario; i Governi dei Paesi membri, almeno in linea programmatica, attraverso azioni politiche e talora legislative, orientano gli amministratori locali a migrare verso i nuovi mezzi di e-*Health*.

Per il raggiungimento dei suddetti obiettivi di trasferimento dati sono, inoltre, predisposte misure formali e *standard* per tutelare la *privacy* e garantire la *security*: si pensi ai meccanismi di autenticazione, identificazione, *audit trail* (particolare attenzione è in questo senso rivolta ai ruoli - di *provider, consumer* e *registry* - assunti dagli attori coinvolti) nonché agli *standard* XACML e RBAC.

Elemento comune a tutti i progetti selezionati è, altresì, l'utilizzo dello *standard Clinical Document Architecture* di "*Health Level 7*", per importare ed esportare dati clinici

[371] In riferimento al contesto europeo la ricerca ha preso in considerazione progetti di tipo nazionale. Tale scelta è stata principalmente condizionata da ragioni linguistiche e dalla non sempre facile reperibilità *online* dei documenti tecnici di interesse.

strutturati tra le applicazioni, consentendo, dunque, un adeguato livello di interoperabilità semantica tra i documenti.

Sebbene le osservazioni proposte siano valide per il campione esaminato, lo scenario, almeno quello italiano locale, che, a tutt'oggi, si presenta è di altra natura, dal momento che, spesso, laddove siano presenti prototipi di FSE, la struttura che il dato e il documento digitale assumono è mera trasposizione del documento cartaceo, in cui i meccanismi di de-identificazione delle informazioni sensibili seguono modalità diverse rispetto ai dati elettronici *machine-readable*[372] (non sempre, infatti, i documenti sanitari sono strutturati secondo lo *standard* HL7 - CDA Rel. 2.0 e sono utilizzati i formati .pdf o . jpg per lo scambio digitale delle informazioni clinico-sanitarie dell'assisito).

La criticità di questo aspetto, è particolarmente rilevante per le implicazioni del presente lavoro, essenzialmente connesse alla possibilità di dare valore alle informazioni sanitarie anche al di fuori dei percorsi diagnostico-terapeutici, attraverso un utilizzo "aperto", per finalità secondarie di ricerca e salute pubblica, dei dati de-identificati raccolti nei FSE.

Verosimilmente risponde a questa esigenza, quella cioè di migliorare in modo efficiente ed efficace i livelli di interoperabilità tra i sistemi informativi sanitari locali, quanto prescritto nelle Linee guida del 31 marzo 2014, che, in merito ai sistemi di codifica dei dati, appunto evidenziano: "*per quanto concerne le strutture informative complesse che costituiscono il nucleo minimo del FSE si adotta lo standard HL7 (Health Level 7) per descrivere le definizioni dei dati da scambiare in termini di messaggi e documenti costituenti il FSE, e in particolare è prescritto l'utilizzo del CDA (Clinical Document Architecture) release 2 (ISO/HL7 27932:2009)*"[373].

Fotografato lo stato dell'arte, obiettivo specifico della ricerca era quello di suggerire nuovi approcci, soprattutto in merito all'utilizzo con finalità secondarie dei dati collezionati nel FSE.

Requisito essenziale per ipotizzare uno scenario in cui i dati collezionati nel FSE siano utilizzabili con finalità di ricerca e salute pubblica è quello della de-identificazione delle informazioni sanitarie.

[372] Non da ultimo, le "Linee guida per la presentazione dei piani di progetto regionali per il FSE" hanno l'obiettivo di fornire una guida tecnica e di indicare i principali modelli di riferimento per la predisposizione dei piani di progetto sulla realizzazione dei sistemi regionali di Fascicolo Sanitario Elettronico (da attivare entro il 30 giugno 2015), come disciplinato dal DPCM in fase di emanazione di cui al comma 7 dell'art. 12 del decreto legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, e successive modificazioni.

[373] Ivi, p. 8.

Quest'evidenza non è scevra di problemi. Infatti, se in letteratura il dibattito sull'efficacia dei meccanismi di de-identificazione (e, soprattutto, possibilità di re-identificazione) è acceso, elevati sono i timori dei giuristi italiani sulla questione dell'identificabilità, anche indiretta, del paziente, che implicherebbe la violazione dell'articolo 4, lettera (b), del "Codice in materia di protezione dei dati personali".

Talune esperienze internazionali indicate nel capitolo IV, rivelano, però, che, nel caso di trattamento di "*big data*", ovvero quantità elevate di informazioni sanitarie, le percentuali di re-identificazione del paziente sono minime.

Benché si sia consapevoli che la protezione dei dati personali non si fondi su percentuali e che sia riconosciuta come diritto inviolabile dell'uomo, si ritiene essenziale tornare a riflettere sul tema in termini di bilanciamento di interessi: diritto alla salute del singolo da una parte ed interesse della collettività dall'altra.

In questo senso, l'utilizzo di meccanismi di identificazione univoca degli assistiti, in forma anonima, cui ricondurre tutti gli eventi sanitari occorsi nel corso della vita, è una possibile soluzione da adottare nella progettazione di sistemi informativi di FSE.

Sebbene, infatti, il FSE sia un *unicum* dal punto di vista concettuale, non bisogna, però, dimenticare che esso è essenzialmente costituito da dati. Escluse le informazioni personali e sensibili, il resto dei dati ha un valore oggettivamente neutro; trattasi di numeri, testi, immagini, suoni, la cui elaborazione può portare alla conoscenza dell'oggetto di indagine e può rivelarsi decisiva sia per i processi diagnostici e di cura del singolo sia per la salute della comunità.

Se è vero che dal punto di vista giuridico non vi è alcun ostacolo al trattamento di dati de-identificati e, dunque, anonimi per finalità secondaria, una sfida interessante è quella di progettare l'infrastruttura tecnologica sul FSE tenendo conto dei principi in materia di "*Open Data*" e "*Linked Open Data*". La *ratio* di tale proposta ha anzitutto motivazioni pratiche: la quantità di dati de-identificati contenuta nei FSE è elevata; la ricerca scientifica si basa su evidenze qualitativamente e quantitativamente significative; estrarre dati, aggregati e non, dai FSE potrebbe aprire a nuovi scenari nel futuro della salute pubblica.

Affinché l'ipotesi avanzata sia quantomeno considerabile è essenziale intervenire, con un processo di armonizzazione, su tre fronti: (1) normativo, (2) di regole tecniche e giuridiche nonché (3) nel *design* degli strumenti informatici e tecnologici.

Le problematiche sottese ad un possibile processo di apertura dell'informazione sanitaria raccolta nel FSE sono, infatti, molteplici e, per taluni profili, distinte da quelle che investono l'apertura dei dati prodotti e detenuti dalla Pubblica Amministrazione.

Al consenso della comunità di esperti nel settore informatico, in particolare, per ciò che concerne il formato dei dati ed il design dei sistemi informativi sanitari, occorre coniugare il consenso del mondo giuridico, non solo per il tema della licenza d'uso, ma, soprattutto, per regolare la materia.

Si ritiene, però, che l'ostacolo principale da superare riguardi l'effettiva de-identificazione dell'informazione sanitaria, la cui realizzazione semplificherebbe la previsione normativa e, ciò, dal momento che, è insito nella stessa natura degli "*Open Data*" l'essere liberamente utilizzati, riutilizzati e re-distribuiti, con la sola eventuale limitazione di attribuzione dell'autore e di un'analoga redistribuzione dei dati.

APPENDICE

Capitolo Secondo

NOTA 87 - Tra gli *standard* ISO/TC 215 già pubblicati rientrano: ISO 1828:2012, "*Health informatics - Categorial structure for terminological systems of surgical procedures*"; ISO 10159:2011, "*Health informatics - Messages and communication - Web access reference manifest*"; ISO/HL7 10781:2009, "*Electronic Health Record-System Functional Model, Release 1.1*"; ISO/IEEE 11073-10101:2004, "*Health informatics - Point-of-care medical device communication - Part 10101: Nomenclature*"; ISO/IEEE 11073-10201:2004, "*Health informatics - Point-of-care medical device communication - Part 10201: Domain information model*"; ISO/IEEE 11073-10404:2010, "*Health informatics - Personal health device communication - Part 10404: Device specialization - Pulse oximeter*"; ISO/IEEE 11073-10406:2012, "*Health informatics - Personal health device communication - Part 10406: Device specialization - Basic electrocardiograph (ECG) (1- to 3-lead ECG)*"; ISO/IEEE 11073-10407:2010, "*Health informatics -Personal health device communication - Part 10407: Device specialization - Blood pressure monitor*"; ISO/IEEE 11073-10408:2010, "*Health informatics - Personal health device communication - Part 10408: Device specialization - Thermometer*"; ISO/IEEE 11073-10415:2010, "*Health informatics - Personal health device communication - Part 10415: Device specialization - Weighing scale*"; ISO/IEEE 11073-10417:2010, "*Health informatics - Personal health device communication - Part 10417: Device specialization - Glucose meter*"; ISO/IEEE 11073-10420:2012, "*Health informatics - Personal health device communication - Part 10420: Device specialization - Body composition analyzer*"; ISO/IEEE 11073-10421:2012, "*Health informatics - Personal health device communication - Part 10421: Device specialization - Peak expiratory flow monitor (peak flow)*"; ISO/IEEE 11073-10471:2010, "*Health informatics - Personal health device communication - Part 10471: Device specialization - Independant living activity hub*"; ISO/IEEE 11073-10472:2012, "*Health Informatics - Personal health device communication - Part 10472: Device specialization - Medication monitor*"; ISO/IEEE 11073-20101:2004, "*Health informatics - Point-of-care medical device communication - Part 20101: Application profiles - Base standard*"; ISO/IEEE 11073-20601:2010, "*Health*

informatics - Personal health device communication - Part 20601: Application profile - Optimized exchange protocol"; ISO/IEEE 11073-30200:2004, "*Health informatics - Point-of-care medical device communication - Part 30200: Transport profile - Cable connected*"; ISO/IEEE 11073-30300:2004, "*Health informatics - Point-of-care medical device communication - Part 30300: Transport profile - Infrared wireless*"; ISO/IEEE 11073-30400:2012, "*Health informatics - Point-of-care medical device communication - Part 30400: Interface profile - Cabled Ethernet*"; ISO 11073-90101:2008, "*Health informatics - Point-of-care medical device communication - Part 90101: Analytical instruments - Point-of-care test*"; ISO 11073-91064:2009, "*Health informatics - Standard communication protocol - Part 91064: Computer-assisted electrocardiography*"; ISO/TS 11073-92001:2007, "*Health informatics - Medical waveform format - Part 92001: Encoding rules*"; ISO 11238:2012, "*Health informatics - Identification of medicinal products - Data elements and structures for the unique identification and exchange of regulated information on substances*"; ISO 11239:2012, "*Health informatics - Identification of medicinal products - Data elements and structures for the unique identification and exchange of regulated information on pharmaceutical dose forms, units of presentation, routes of administration and packaging*"; ISO 11240:2012, "*Health informatics - Identification of medicinal products - Data elements and structures for the unique identification and exchange of units of measurement*"; ISO/TR 11487:2008, "*Health informatics - Clinical stakeholder participation in the work of ISO TC 215*"; ISO 11615:2012, "*Health informatics - Identification of medicinal products - Data elements and structures for the unique identification and exchange of regulated medicinal product information*"; ISO 11616:2012, "*Health informatics - Identification of medicinal products - Data elements and structures for the unique identification and exchange of regulated pharmaceutical product information*"; ISO/TR 11633-1:2009, "*Health informatics - Information security management for remote maintenance of medical devices and medical information systems - Part 1: Requirements and risk analysis*"; ISO/TR 11633-2:2009, "*Health informatics - Information security management for remote maintenance of medical devices and medical information systems - Part 2: Implementation of an information security management system (ISMS)*"; ISO/TR 11636:2009, "*Health Informatics - Dynamic on-demand virtual private network for health information infrastructure*"; ISO 12052:2006, "*Health informatics - Digital imaging and communication in medicine (DICOM) including workflow and data management*"; ISO/TR 12309:2009, "*Health informatics - Guidelines for terminology development organizations*"; ISO/TR 12773-

1:2009, "*Business requirements for health summary records - Part 1: Requirements*"; ISO/TR 12773-2:2009, "*Business requirements for health summary records - Part 2: Environmental scan*"; ISO 12967-1:2009, "*Health informatics - Service architecture - Part 1: Enterprise viewpoint*"; ISO 12967-2:2009, "*Health informatics - Service architecture - Part 2: Information viewpoint*"; ISO 12967-3:2009, "*Health informatics - Service architecture - Part 3: Computational viewpoint*"; ISO/TR 13054:2012, "*Knowledge management of health information standards*"; ISO 13119:2012, "*Health informatics - Clinical knowledge resources – Metadata*"; ISO/TR 13128:2012, "*Health Informatics - Clinical document registry federation*"; ISO/TS 13582:2013, "*Health informatics - Sharing of OID registry information*"; ISO 13606-1:2008, "*Health informatics - Electronic health record communication - Part 1: Reference model*"; ISO 13606-2:2008, "*Health informatics - Electronic health record communication - Part 2: Archetype interchange specification*"; ISO 13606-3:2009, "*Health informatics - Electronic health record communication - Part 3: Reference archetypes and term lists*"; ISO/TS 13606-4:2009, "*Health informatics - Electronic health record communication - Part 4: Security*"; ISO 13606-5:2010, "*Health informatics - Electronic health record communication - Part 5: Interface specification*"; ISO/TS 14265:2011, "*Health Informatics - Classification of purposes for processing personal health information*"; ISO/TR 14292:2012, "*Health informatics - Personal health records - Definition, scope and context*"; ISO/TR 14639-1:2012, "*Health informatics - Capacity-based eHealth architecture roadmap - Part 1: Overview of national eHealth initiatives*"; ISO/TR 16056-1:2004, "*Health informatics - Interoperability of telehealth systems and networks - Part 1: Introduction and definitions*"; ISO/TR 16056-2:2004, "*Health informatics - Interoperability of telehealth systems and networks - Part 2: Real-time systems*"; ISO/TS 16058:2004, "*Health informatics - Interoperability of telelearning systems*"; ISO 17090-1:2008, "*Health informatics - Public key infrastructure - Part 1: Overview of digital certificate services*"; ISO 17090-2:2008, "*Health informatics - Public key infrastructure - Part 2: Certificate profile*"; ISO 17090-3:2008, "*Health informatics - Public key infrastructure - Part 3: Policy management of certification authority*"; ISO 17115:2007, "*Health informatics - Vocabulary for terminological systems*"; ISO/TS 17117:2002, "*Health informatics - Controlled health terminology - Structure and high-level indicators*"; ISO/TR 17119:2005, "*Health informatics - Health informatics profiling framework*"; ISO 17432:2004, "*Health informatics - Messages and communication - Web access to DICOM persistent objects*"; ISO 18104:2003, "*Health informatics - Integration of a reference terminology model for*

nursing"; ISO 18232:2006, "*Health Informatics - Messages and communication - Format of length limited globally unique string identifiers*"; ISO/TR 18307:2001, "*Health informatics - Interoperability and compatibility in messaging and communication standards - Key characteristics*"; ISO 18308:2011, "*Health informatics - Requirements for an electronic health record architecture*"; ISO 18812:2003, "*Health informatics - Clinical analyser interfaces to laboratory information systems - Use profiles*"; ISO 20301:2006, "*Health informatics - Health cards - General characteristics*"; ISO 20302:2006, "*Health informatics - Health cards - Numbering system and registration procedure for issuer identifiers*"; ISO/TR 20514:2005, "*Health informatics - Electronic health record - Definition, scope and context*"; ISO/TR 21089:2004, "*Health informatics - Trusted end-to-end information flows*"; ISO 21090:2011, "*Health informatics - Harmonized data types for information interchange*"; ISO 21091:2013, "*Health informatics - Directory services for healthcare providers, subjects of care and other entities*"; ISO/TS 21298:2008, "Health informatics - Functional and structural roles"; ISO/TS 21547:2010, "*Health informatics - Security requirements for archiving of electronic health records - Principles*"; ISO/TR 21548:2010, "*Health informatics - Security requirements for archiving of electronic health records - Guidelines*"; ISO 21549-1:2004, "*Health informatics - Patient healthcard data - Part 1: General structure*"; ISO 21549-2:2004, "*Health informatics - Patient healthcard data - Part 2: Common objects*"; ISO 21549-3:2004, "*Health informatics - Patient healthcard data - Part 3: Limited clinical data*"; ISO 21549-4:2006, "*Health informatics - Patient healthcard data - Part 4: Extended clinical data*"; ISO 21549-5:2008, "*Health informatics - Patient healthcard data - Part 5: Identification data*"; ISO 21549-6:2008, "*Health informatics - Patient healthcard data - Part 6: Administrative data*"; ISO 21549-7:2007, "*Health informatics - Patient healthcard data - Part 7: Medication data*"; ISO 21549-8:2010, "*Health informatics - Patient healthcard data - Part 8: Links*"; ISO 21667:2010, "*Health informatics - Health indicators conceptual framework*"; ISO/TR 21730:2007, "*Health informatics - Use of mobile wireless communication and computing technology in healthcare facilities - Recommendations for electromagnetic compatibility (management of unintentional electromagnetic interference) with medical devices*"; ISO/HL7 21731:2006, "*Health informatics - HL7 version 3 - Reference information model - Release 1*"; ISO/TS 22220:2011, "*Health informatics - Identification of subjects of health care*"; ISO/TR 22221:2006, "*Health informatics - Good principles and practices for a clinical data warehouse*"; ISO/TS 22224:2009, "*Health informatics - Electronic reporting of adverse drug reactions*"; ISO/TS 22600-1:2006, "*Health informatics - Privilege*

management and access control - Part 1: Overview and policy management"; ISO/TS 22600-2:2006, "*Health informatics - Privilege management and access control - Part 2: Formal models*"; ISO/TS 22600-3:2009, "*Health informatics - Privilege management and access control - Part 3: Implementations*"; ISO/TS 22789:2010, "*Health informatics - Conceptual framework for patient findings and problems in terminologies*"; ISO/TR 22790:2007, "*Health informatics - Functional characteristics of prescriber support systems*"; ISO 22857:2004, "*Health informatics - Guidelines on data protection to facilitate trans-border flows of personal health information*"; ISO/TS 25237:2008, "*Health informatics - Pseudonymization*"; ISO/TS 25238:2007, "*Health informatics - Classification of safety risks from health software*"; ISO/TR 25257:2009, "*Health informatics - Business requirements for an international coding system for medicinal product*"; ISO 25720:2009, "*Health informatics - Genomic Sequence Variation Markup Language (GSVML)*"; ISO/TS 27527:2010, "*Health informatics - Provider identification*"; ISO 27789:2013, "*Health informatics - Audit trails for electronic health records*"; ISO/TS 27790:2009, "*Health informatics - Document registry framework*"; ISO 27799:2008, "*Health informatics - Information security management in health using ISO/IEC 27002*"; ISO/TR 27809:2007, "*Health informatics - Measures for ensuring patient safety of health software*"; ISO/HL7 27931:2009, "*Data Exchange Standards - Health Level Seven Version 2.5 - An application protocol for electronic data exchange in healthcare environments*"; ISO/HL7 27932:2009, "*Data Exchange Standards - HL7 Clinical Document Architecture, Release 2*"; ISO/HL7 27951:2009, "*Health informatics - Common terminology services, release 1*"; ISO/HL7 27953-1:2011, "*Health informatics - Individual case safety reports (ICSRs) in pharmacovigilance - Part 1: Framework for adverse event reporting*"; ISO/HL7 27953-2:2011, "*Health informatics - Individual case safety reports (ICSRs) in pharmacovigilance - Part 2: Human pharmaceutical reporting requirements for ICSR*"; ISO/TS 29585:2010, "*Health informatics - Deployment of a clinical data warehouse*"; IEC 80001-1:2010, "*Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities*"; IEC/TR 80001-2-1:2012, "*Application of risk management for IT-networks incorporating medical devices - Part 2-1: Step by Step Risk Management of Medical IT-Networks; Practical Applications and Examples*"; IEC/TR 80001-2-2:2012, "*Application of risk management for IT-networks incorporating medical devices - Part 2-2: Guidance for the communication of medical device security needs, risks and controls*"; IEC/TR 80001-2-3:2012, "*Application of risk management for IT-networks incorporating medical devices - Part 2-3: Guidance for*

wireless networks"; IEC/TR 80001-2-4:2012, "*Application of risk management for IT-networks incorporating medical devices - Part 2-4: General implementation guidance for Healthcare Delivery Organizations*".

NOTA 90 - *Standard* pubblicati da CEN/TC 251 sono: CEN/TR 15212:2006, "*Health informatics - Vocabulary - Maintenance procedure for a web-based terms and concepts database*"; CEN/TR 15253:2005, "*Health informatics - Quality of service requirements for health information interchange*"; CEN/TR 15299:2006, "*Health informatics - Safety procedures for identification of patients and related objects*"; CEN/TR 15300:2006, "*Health informatics - Framework for formal modelling of healthcare security policies*"; CEN/TR 15640:2007, "*Health informatics - Measures for ensuring the patient safety of health software*"; CEN/TS 14822-4:2005, "*Health informatics - General purpose information components - Part 4: Message headers*"; CEN/TS 15260:2006, "*Health informatics - Classification of safety risks from health informatics products*"; CR 12161:1995, "*A method for defining profiles for healthcare*"; CR 12587:1996, "*Medical Informatics - Methodology for the development of healthcare messages*"; CR 1350:1993, "*Investigation of syntaxes for existing interchange formats to be used in health care*"; CR 13694:1999, "*Health Informatics - Safety and Security Related Software Quality Standards for Healthcare (SSQS)*"; CR 14301:2002, "*Health informatics - Framework for security protection of healthcare communication*"; CR 14302:2002, "*Health informatics - Framework for security requirements for intermittently connected devices*"; EN 1064:2005+A1:2007, "*Health informatics - Standard communication protocol - Computer-assisted electrocardiography*"; EN 1068:2005, "*Health informatics - Registration of coding systems*"; EN 12251:2004, "*Health informatics - Secure User Identification for Health Care - Management and Security of Authentication by Passwords*"; EN 12264:2005, "*Health informatics - Categorial structures for systems of concepts*"; EN 12381:2005, "*Health informatics - Time standards for healthcare specific problems*"; EN 12435:2006, "*Health informatics - Expression of results of measurements in health sciences*"; EN 13606-2:2007, "*Health informatics - Electronic health record communication - Part 2: Archetypes interchange specification*"; EN 13606-3:2008, "*Health informatics - Electronic health record communication - Part 3: Reference archetypes and term lists*"; EN 13606-4:2007, "*Health informatics - Electronic health record communication - Part 4: Security*"; EN 13609-1:2005, "*Health informatics -*

Messages for maintenance of supporting information in healthcare systems - Part 1: Updating of coding schemes"; EN 13940-1:2007, "*Health informatics - System of concepts to support continuity of care - Part 1: Basic concepts*"; EN 14463:2007, "*Health informatics - A syntax to represent the content of medical classification systems - ClaML*"; EN 14484:2003, "*Health informatics - International transfer of personal health data covered by the EU data protection directive - High level security policy*"; EN 14485:2003, "*Health informatics - Guidance for handling personal health data in international applications in the context of the EU data protection directive*"; EN 14822-1:2005, "*Health informatics - General purpose information components - Part 1: Overview*"; EN 14822-2:2005, "*Health informatics - General purpose information components - Part 2: Non-clinical*"; EN 14822-3:2005, "*Health informatics - General purpose information components - Part 3: Clinical*"; EN 15521:2007, "*Health informatics - Categorial structure for terminologies of human anatomy*"; EN 1614:2006, "*Health informatics - Representation of dedicated kinds of property in laboratory medicine*"; EN ISO 10781:2009, "*Electronic Health Record-System Functional Model, Release 1.1 (ISO 10781:2009)*"; EN ISO 11073-10101:2005, "*Health informatics - Point-of-care medical device communication - Part 10101: Nomenclature (ISO/IEEE 11073-10101:2004)*"; EN ISO 11073-10201:200, "*Health informatics - Point-of-care medical device communication - Part 10201: Domain information model (ISO/IEEE 11073-10201:2004)*"; EN ISO 11073-10404:2011, "*Health informatics - Personal health device communication - Part 10404: Device specialization - Pulse oximeter (ISO/IEEE 11073-10404:2010)*"; EN ISO 11073-10406:2012, "*Health informatics - Personal health device communication - Part 10406: Device specialization - Basic electrocardiograph (ECG) (1- to 3-lead ECG) (ISO/IEEE 11073-10406:2012)*"; EN ISO 11073-10407:2011, "*Health informatics - Personal health device communication - Part 10407: Device specialization - Blood pressure monitor (ISO/IEEE 11073-10407:2010)*"; EN ISO 11073-10408:2011, "*Health informatics - Personal health device communication - Part 10408: Device specialization - Thermometer (ISO/IEEE 11073-10408:2010)*"; EN ISO 11073-10415:2011, "*Health informatics - Personal health device communication - Part 10415: Device specialization - Weighing scale (ISO/IEEE 11073-10415:2010)*"; EN ISO 11073-10417:2011, "*Health informatics - Personal health device communication - Part 10417: Device specialization - Glucose meter (ISO/IEEE 11073-10417:2010)*"; EN ISO 11073-10420:2012, "*Health informatics - Personal health device communication - Part 10420: Device specialization - Body composition analyzer (ISO 11073-10420:2012)*"; EN ISO 11073-10421:2012,

"*Health informatics - Personal health device communication - Part 10421: Device specialization - Peak expiratory flow monitor (peak flow) (ISO 11073-10421:2012)*"; EN ISO 11073-10471:2011, "*Health Informatics - Personal health device communication - Part 10471: Device specialization - Independant living activity hub (ISO/IEEE 11073-10471:2010)*"; EN ISO 11073-10472:2012, "*Health Informatics - Personal health device communication - Part 10472: Device specialization - Medication monitor (ISO 11073-10472:2012)*"; EN ISO 11073-20101:2005, "*Health informatics - Point-of-care medical device communication - Part 20101: Application profiles - Base standard (ISO/IEEE 11073-20101:2004)*"; EN ISO 11073-20601:2011, "*Health informatics - Personal health device communication - Part 20601: Application profile - Optimized exchange protocol (ISO/IEEE 11073-20601:2010)*"; EN ISO 11073-30200:2005, "*Health informatics - Point-of-care medical device communication - Part 30200: Transport profile - Cable connected (ISO/IEEE 11073-30200:2004)*"; EN ISO 11073-30300:2005, "*Health informatics - Point-of-care medical device communication - Part 30300: Transport profile - Infrared wireless (ISO/IEEE 11073-30300:2004)*"; EN ISO 11073-30400:2012, "*Health informatics - Point-of-care medical device communication - Part 30400: Interface profile - Cabled Ethernet (ISO 11073-30400:2012)*"; EN ISO 11238:2012, "*Health informatics - Identification of medicinal products - Data elements and structures for the unique identification and exchange of regulated information on substances (ISO 11238:2012)*"; EN ISO 11239:2012, "*Health informatics - Identification of medicinal products - Data elements and structures for the unique identification and exchange of regulated information on pharmaceutical dose forms, units of presentation, routes of administration and packaging (ISO 11239:2012)*"; EN ISO 11240:2012, "*Health informatics - Identification of medicinal products - Data elements and structures for the unique identification and exchange of units of measurement (ISO 11240:2012)*"; EN ISO 11615:2012, "*Health informatics - Identification of medicinal products - Data elements and structures for the unique identification and exchange of regulated medicinal product information (ISO 11615:2012)*"; EN ISO 11616:2012, "*Health informatics - Identification of medicinal products - Data elements and structures for the unique identification and exchange of regulated pharmaceutical product information (ISO 11616:2012)*"; EN ISO 12052:2011, "*Health informatics - Digital imaging and communication in medicine (DICOM) including workflow and data management (ISO 12052:2006)*"; EN ISO 12967-1:2011, "*Health informatics - Service architecture - Part 1: Enterprise viewpoint (ISO 12967-1:2009)*"; EN ISO 12967-2:2011, "*Health informatics - Service architecture - Part 2: Information*

viewpoint (ISO 12967-2:2009)"; EN ISO 12967-3:2011, "*Health informatics - Service architecture - Part 3: Computational viewpoint (ISO 12967-3:2009)*"; EN ISO 13119:2012, "*Health informatics - Clinical knowledge resources - Metadata (ISO 13119:2012)*"; EN ISO 13606-1:2012, "*Health informatics - Electronic health record communication - Part 1: Reference model (ISO 13606-1:2008)*"; EN ISO 13606-5:2010, "*Health informatics - Electronic health record communication - Part 5: Interface specification (ISO 13606-5:2010)*"; EN ISO 18104:2003, "*Health Informatics - Integration of a reference terminology model for nursing (ISO 18104:2003)*"; EN ISO 1828:2012, "*Health informatics - Categorial structure for terminological systems of surgical procedures (ISO 1828:2012)*"; EN ISO 18812:2003, "*Health informatics - Clinical analyser interfaces to laboratry information systems - Use profiles (ISO 18812:2003)*"; EN ISO 21090:2011, "*Health Informatics - Harmonized data types for information interchange (ISO 21090:2011)*"; EN ISO 21091:2013, "*Health informatics - Directory services for healthcare providers, subjects of care and other entities (ISO 21091:2013)*"; EN ISO 21549-1:2004, "*Health informatics - Patient healthcard data - Part 1: General structure (ISO 21549-1:2004)*"; EN ISO 21549-2:2004, "*Health informatics - Patient healthcard data - Part 2: Common objects (ISO 21549-2:2004)*"; EN ISO 21549-3:2004, "*Health informatics - Patient healthcard data - Part 3: Limited clinical data (ISO 21549-3:2004)*"; EN ISO 21549-4:2006, "*Health informatics - Patient healthcard data - Part 4: Extended clinical data (ISO 21549-4:2006)*"; EN ISO 21549-5:2008, "*Health informatics - Patient healthcard data - Part 5: Identification data (ISO 21549-5:2008)*"; EN ISO 21549-6:2008, "*Health informatics - Patient healthcard data - Part 6: Administrative data (ISO 21549-6:2008)*"; EN ISO 21549-7:2007, "*Health informatics - Patient healthcard data - Part 7: Medication data (ISO 21549-7:2007)*"; EN ISO 21549-8:2010, "*Health informatics - Patient healthcard data - Part 8: Links (ISO 21549-8:2010)*"; EN ISO 27789:2013, "*Health informatics - Audit trails for electronic health records (ISO 27789:2013)*"; EN ISO 27799:2008, "*Health informatics - Information security management in health using ISO/IEC 27002 (ISO 27799:2008)*"; EN ISO 27953-1:2011, "*Health informatics - Individual case safety reports (ICSRs) in pharmacovigilance - Part 1: Framework for adverse event reporting (ISO 27953-1:2011)*"; EN ISO 27953-2:2011, "*Health informatics - Individual case safety reports (ICSRs) in pharmacovigilance - Part 2: Human pharmaceutical reporting requirements for ICSR (ISO 27953-2:2011)*"; ENV 12443:1999, "*Medical Informatics - Healthcare Information Framework (HIF)*"; ENV 12537-1:1997, "*Medical informatics - Registration of information objects used for EDI in healthcare -*

Part 1: The Register"; ENV 12610:1997, "*Medical informatics - Medicinal product identification -*"; ENV 12611:1997, "*Medical informatics - Categorial structure of systems of concepts - Medical devices*"; ENV 12612:1997, "*Medical informatics - Messages for the exchange of healthcare administrative information*"; ENV 13607:2000, "*Health informatics - Messages for the exchange of information on medicine prescriptions*"; ENV 13609-2:2000, "*Health informatics - Messages for maintenance of supporting information in healthcare systems - Part 2: Updating of medical laboratory-specific information*"; ENV 13730-1:2001, "*Health informatics - Blood transfusion related messages - Part 1: Subject of care related messages*"; ENV 13730-2:2002, "*Healthcare Informatics - Blood transfusion related messages - Part 2: Production related messages (BTR-PROD)*".

NOTA 98 - *Standard* della famiglia ISO/IEEE 11073 sono: ISO/IEEE 11073-10101:2004, "*Health informatics - Point-of-care medical device communication - Part 10101: Nomenclature*"; ISO/IEEE 11073-10201:2004, "*Health informatics - Point-of-care medical device communication - Part 10201: Domain information model*"; ISO/IEEE 11073-10404:2010, "*Health informatics - Personal health device communication - Part 10404: Device specialization - Pulse oximeter*"; ISO/IEEE 11073-10406:2012, "*Health informatics - Personal health device communication - Part 10406: Device specialization - Basic electrocardiograph (ECG) (1- to 3-lead ECG)*"; ISO/IEEE 11073-10407:2010, "*Health informatics - Personal health device communication - Part 10407: Device specialization - Blood pressure monitor*"; ISO/IEEE 11073-10408:2010, "*Health informatics - Personal health device communication - Part 10408: Device specialization - Thermometer*"; ISO/IEEE 11073-10415:2010, "*Health informatics - Personal health device communication - Part 10415: Device specialization - Weighing scale*", ISO/IEEE 11073-10417:2010, "*Health informatics - Personal health device communication - Part 10417: Device specialization - Glucose meter*"; ISO/IEEE DIS 11073-10417, "*Health informatics - Personal health device communication - Part 10417: Device specialization - Glucose meter*"; ISO/IEEE DIS 11073-10418, "*Health informatics - Personal health device communication - Part 10418: Device specialization-International Normalized Ratio (INR) monitor*"; ISO/IEEE 11073-10420:2012, "*Health informatics - Personal health device communication - Part 10420: Device specialization - Body composition analyzer*"; ISO/IEEE 11073-10421:2012, "*Health informatics - Personal health device communication - Part 10421: Device specialization - Peak expiratory flow monitor (peak flow)*"; ISO/IEEE 11073-10471:2010, "*Health informatics - Personal health device*

communication - Part 10471: Device specialization - Independant living activity hub"; ISO/IEEE 11073-10472:2012, "*Health Informatics - Personal health device communication - Part 10472: Device specialization - Medication monitor*"; ISO/IEEE 11073-20101:2004, "*Health informatics - Point-of-care medical device communication - Part 20101: Application profiles - Base standard*"; ISO/IEEE 11073-20601:2010, "*Health informatics - Personal health device communication - Part 20601: Application profile - Optimized exchange protocol*"; ISO/IEEE 11073-30200:2004, "*Health informatics - Point-of-care medical device communication - Part 30200: Transport profile - Cable connected*"; ISO/IEEE 11073-30300:2004, "*Health informatics - Point-of-care medical device communication - Part 30300: Transport profile - Infrared wireless*"; ISO/IEEE 11073-30400:2012, "*Health informatics - Point-of-care medical device communication - Part 30400: Interface profile - Cabled Ethernet*".

NOTA 102 – Di seguito si riportano gli Stati (e le organizzazioni nazionali coinvolte) aderenti al Progetto "*Smart Open Services for European Patients*", dei quali, venti appartengono all'Unione europea e tre non sono Paesi membri: Austria (*Austrian Federal Ministry of Health, ELGA*), Belgio (*Plate-forme eHealth* (BEPLAT), *RECIP-E VZW, Integrating the Healthcare Enterprise-Europe AISBL* (IHE)), Repubblica Ceca (*Internet Access to Patient Electronic Health Record* (IZIP)), Danimarca (*Danish National Board of e-Health, Indenrigs- og Sundhedsministeriet*, *Danish National Health Data Network* (MEDCOM)[374]), Estonia (*Eesti e-Tervise Sihtasutus* (EESTI)), Finlandia (*Terveyden Ja Hyvinvoinnin Laitos* (THL)), Francia (*French Ministry of Health*, *ASIP Santé* (*Agence des systèmes d'information partagés de santé*)), Germania (*German Federal Ministry of Health, Fraunhofergesellschaft zur Förderung der angewandten Forschung* (Fraunhofer ISST), *Gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH*, *Zentralinstitut für die kassenärztliche Versorgung* (ZI), *Empirica Gesellschaft für Kommunikations - und Technologieforschung mbH* (EMPIRICA)), Grecia (*Pharmaxis, Aristotelean University of Thessaloniki*), Ungheria (*Egeszsegugyi Strategiai Kutatointezet* (ESKI)), Italia (Regione Lombardia, Lombardia Informatica (LISPA)), Malta (*Ministry for Health, the Elderly and Community Care* (MHEC)), Norvegia (*Helsedirektorate* (NONA), *Kompetansesenter for Informasjonsteknologi i Helsevesenet as* (KITH)), Polania (*Narodowy Fundusz Zdrowia* (NFZ), *Instytut Logistyki I Magazynowania* (ILIM)),

[374] MedCom ha aderito al Progetto epSOS fino a dicembre 2010.

Portugallo (*Administração Central do Sistema de Saúde, I.P.* (PTNA), *Universidade de Aveiro* (UAVR)), Slovenia (*Institut Za Varovanje Zdravja Republike Slovenije* (NIPHRS)), Slovacchia (*National Health Information Centre* (NHIC)), Spagna (*Spanish Ministry of Health and Consumer Affairs*, *Fundació TicSalut Catalonia*, *Regional Healthcare Service of Andalucia*, *Regional Healthcare Service of Castilla La Mancha* (SESCAM), *Catalan Agency for Health Information, Assessment and Quality* (AIAQS), *Agencia Valenciana de Salud* (AVS), *Servei de Salut de les Illes Balears* (BAL)), Svezia (*Swedish Association of Local Authorities and Regions* (SALAR), *Swedish Ministry of Health and Social Affairs*), Svizzera (*Les Hopitaux Universitaires de Geneve* (HUG), *Federal Office of Public Health* (CHNA)), Paesi Bassi (*National IT Institute for Healthcare in the Netherlands* (NICTIZ), *Dutch Ministry of Health, Welfare and Sport*), Turchia (*Turkiye Cumhuriyeti Saglik Bakanligi* (TRNA), *Srdc Yzilim Arastirma ve Gelistirme ve Danismanlikticaret Limited Sirketi* (SRDC)), Regno Unito (*Department of Health*).

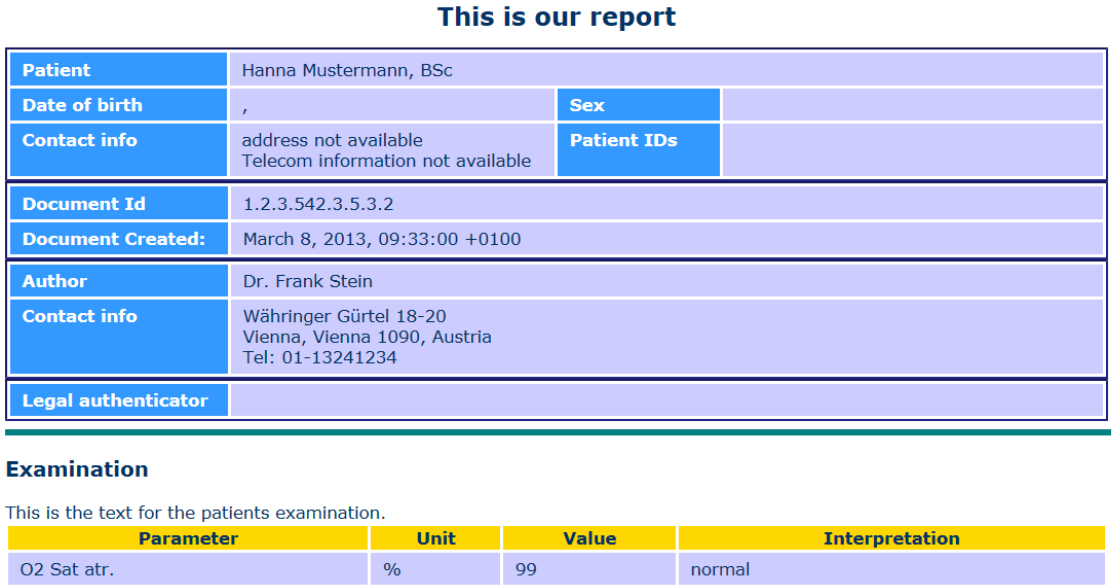
NOTA 138 - Si riporta un esempio, alquanto semplificato, di documento redatto tenendo presente le indicazioni di HL7 CDA; segue, poi, la visualizzazione dello stesso documento secondo il foglio di stile adottato nel progetto ELGA.

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type="text/xsl" href="cda_modular.xsl"?>
<ClinicalDocument xmlns="urn:hl7-org:v3"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:lab="urn:oid:1.3.6.1.4.1.19376.1.3.2" xsi:schemaLocation="urn:hl7-org:v3
CDA.xsd">
        <id root="1.2.3.542.3.5.3.2" extention="asdfasd"/>
        <code code="11502-2" codeSystem="2.16.840.1.113883.6.1"
                displayName="Laboratory report.total" codeSystemName="LOINC"/>
        <effectiveTime value="20130308093300+0100"/>
        <title>This is our report</title>
        <confidentialityCode code="N" codeSystem="2.16.840.1.113883.5.25"
                displayName="normal" codeSystemName="HL7:Confidentiality"/>
        <legalAuthenticator>
                <!- ... ->
        </legalAuthenticator>
```

```
<author>
        <effectiveTime value="20130308084500+0100"/>
        <assignedAuthor>
                <id root="1.2.3.542.3.5.3.2" extention="12431234"/>
                <addr>
                        <streetName>Währinger Gürtel</streetName>
                        <houseNumber>18-20</houseNumber>
                        <postalCode>1090</postalCode>
                        <city>Vienna</city>
                        <state>Vienna</state>
                        <country>Austria</country>
                </addr>
                <telecom value="tel:01-13241234"/>
                <assignedPerson>
                        <name>Dr. Frank Stein</name>
                </assignedPerson>
        </assignedAuthor>
</author>
<recordTarget>
        <patientRole>
                <patient>
                        <name>
                                <given>Hanna</given>
                                <family>Mustermann</family>
                                <family qualifier="BR">VorDerHeirat</family>
                                <suffix qualifier="AC">BSc</suffix>
                                <suffix qualifier="AC">MBA</suffix>
                        </name>
                </patient>
        </patientRole>
</recordTarget>
<component typeCode="COMP">
        <structuredBody classCode="DOCBODY">
                <component typeCode="COMP">
```

```
<section classCode="DOCSECT">
        <title>Examination</title>
        <text>This is the text for the patients
                examination.
                <table>
                        <thead>
                                <row>
                                        <th>Parameter</th>
                                        <th>Unit</th>
                                        <th>Value</th>
                                </row>
                        </thead>
                        <tbody>
                                <row>
                                        <td>O2</td>
                                        <td>%</td>
                                        <td>99</td>
                                </row>
                        </tbody>
                </table>
        </text>
        <entry>
                <observation>
                        <code code="2708-6"
                codeSystem="2.16.840.1.113883.6.1"/>
                        <text>O2 Saturation art.</text>
                        <statusCode code="completed"/>
                        <value xsi:type="PQ" value="99"
                        unit="%"/>
                        <interpretationCode code="N"
codeSystemName="HL7:ObservationInterpretation"
codeSystem="2.16.840.1.113883.5.83"
displayName="normal"/>
                </observation>
```

```
                    </entry>
                </section>
            </component>
        </structuredBody>
    </component>
</ClinicalDocument>
```



This is our report

Patient	Hanna Mustermann, BSc		
Date of birth	,	**Sex**	
Contact info	address not available Telecom information not available	**Patient IDs**	
Document Id	1.2.3.542.3.5.3.2		
Document Created:	March 8, 2013, 09:33:00 +0100		
Author	Dr. Frank Stein		
Contact info	Währinger Gürtel 18-20 Vienna, Vienna 1090, Austria Tel: 01-13241234		
Legal authenticator			

Examination

This is the text for the patients examination.

Parameter	Unit	Value	Interpretation
O2 Sat atr.	%	99	normal

Figura 19 - ELGA *StyleSheet*

Capitolo Terzo

NOTA 198 - *Standard* della famiglia ISO/IEC 27000, "*Information technology - Security techniques - Information security management systems*", sono: ISO/IEC 27000:2012, *Information technology - Security techniques - Information security management systems - Overview and vocabulary*; ISO/IEC 27001:2005, *Information technology - Security techniques - Information security management systems – Requirements*; ISO/IEC DIS 27001, *Information technology - Security techniques - Information security management systems – Requirements*; ISO/IEC DIS 27002, *Information technology - Security techniques - Code of practice for information security controls*; ISO/IEC 27002:2005, *Information technology - Security techniques - Code of practice for information security management*; ISO/IEC 27003:2010, *Information technology - Security techniques - Information security management system implementation guidance*; ISO/IEC 27004:2009,

Information technology - Security techniques - Information security management - Measurement; ISO/IEC 27005:2011, *Information technology - Security techniques - Information security risk management*; ISO/IEC 27006:2011, *Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems*; ISO/IEC WD 27006, *Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems*; ISO/IEC 27007:2011, *Information technology - Security techniques - Guidelines for information security management systems auditing*; ISO/IEC TR 27008:2011, *Information technology - Security techniques - Guidelines for auditors on information security controls*; ISO/IEC NP 27009, *The Use and Application of ISO/IEC 27001 for Sector/Service-Specific Third-Party Accredited Certifications*; ISO/IEC 27010:2012, *Information technology - Security techniques - Information security management for inter-sector and inter-organizational communications*; ISO/IEC 27011:2008, *Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*; ISO/IEC 27013:2012, *Information technology - Security techniques - Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*; ISO/IEC 27011:2008, *Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*; ISO/IEC 27013:2012, *Information technology - Security techniques - Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*; ISO/IEC FDIS 27014, *Information technology - Security techniques - Governance of information security*; ISO/IEC TR 27015:2012, *Information technology - Security techniques - Information security management guidelines for financial services*; ISO/IEC PDTR 27016, *Information technology - Security techniques - Information security management - Organizational economics*; ISO/IEC WD 27017, *Information technology - Security techniques - Information security management - Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002*; ISO/IEC WD 27018, *Code of practice for data protection controls for public cloud computing services*; ISO/IEC DTR 27019, *Information technology - Security techniques - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry*; ISO/IEC 27031:2011, *Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity*; ISO/IEC 27032:2012, *Information technology - Security techniques - Guidelines for cybersecurity*;

ISO/IEC WD 27033-1, *Information technology - Security techniques - Network security - Part 1: Overview and concepts*; ISO/IEC 27033-1:2009, *Information technology - Security techniques - Network security - Part 1: Overview and concepts*; ISO/IEC 27033-2:2012, *Information technology - Security techniques - Network security - Part 2: Guidelines for the design and implementation of network security*; ISO/IEC 27033-3:2010, Information *technology - Security techniques - Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues*; ISO/IEC DIS 27033-4, *Information technology - Security techniques - Network security - Part 4: Securing communications between networks using security gateways*; ISO/IEC DIS 27033-5, *Information technology - Security techniques - Network security - Part 5: Securing communications across networks using Virtual Private Network (VPNs)*; ISO/IEC WD 27033-6, *Information technology - Security techniques - Network security - Part 6: Securing IP network access using wireless*; ISO/IEC 27034-1:2011, *Information technology - Security techniques - Application security - Part 1: Overview and concepts*; ISO/IEC WD 27034-2, *Application security - Part 2: Organization normative framework*; ISO/IEC NP 27034-3, *Application security - Part 3: Application security management process*; ISO/IEC NP 27034-4, *Application security - Part 4: Application security validation*; ISO/IEC WD 27034-5, *Application security - Part 5: Protocols and application security controls data structure*; ISO/IEC WD 27034-6, *Application security - Part 6: Security guidance for specific applications*; ISO/IEC 27035:2011, *Information technology - Security techniques - Information security incident management*; ISO/IEC WD 27035-1, *Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management*; ISO/IEC WD 27035-2, *Information technology - Security techniques - Information security incident management - Part 2: Guidelines for incident response readiness*; ISO/IEC WD 27035-3, *Information technology - Security techniques - Information security incident management - Part 3: Guidelines for CSIRT operations*; ISO/IEC DIS 27036-1, *Information technology - Security techniques - Information security for supplier relationships - Part 1: Overview and concepts*; ISO/IEC DIS 27036-2, *Information technology - Security techniques - Information security for supplier relationships - Part 2: Common requirements*; ISO/IEC DIS 27036-3, *Information technology - Security techniques - Information security for supplier relationships - Part 3: Guidelines for ICT supply chain security*; ISO/IEC WD 27036-4, *Information technology - Security techniques - Information security for supplier relationships - Part 4: Guidelines for security of outsourcing*; ISO/IEC 27037:2012, *Information technology - Security*

techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence; ISO/IEC DIS 27038; *Information technology - Security techniques - Specification for Digital Redaction*; ISO/IEC CD 27039, *Information technology - Security techniques - Selection, deployment and operations of intrusion detection systems*; ISO/IEC CD 27040, *Information technology - Security techniques - Storage security*; ISO/IEC CD 27041, *Guidance on assuring suitability and adequacy of investigation methods*; ISO/IEC CD 27042, *Guidelines for the analysis and interpretation of digital evidence; ISO/IEC CD 27043, Investigation principles and processes*; ISO/IEC WD 27044, *Security Information and Event Management (SIEM)*.

NOTA 220 – L'articolo 23, "Protezione fin dalla progettazione e protezione di defualt", della "Proposta di Regolamento del parlamento europeo e del consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)", così dispone: "1. Al momento di determinare i mezzi del trattamento e all'atto del trattamento stesso, il responsabile del trattamento, tenuto conto dell'evoluzione tecnica e dei costi di attuazione, mette in atto adeguate misure e procedure tecniche e organizzative in modo tale che il trattamento sia conforme al presente regolamento e assicuri la tutela dei diritti dell'interessato. 2. Il responsabile del trattamento mette in atto meccanismi per garantire che siano trattati, di default, solo i dati personali necessari per ciascuna finalità specifica del trattamento e che, in particolare, la quantità dei dati raccolti e la durata della loro conservazione non vadano oltre il minimo necessario per le finalità perseguite. In particolare detti meccanismi garantiscono che, di default, non siano resi accessibili dati personali a un numero indefinito di persone. 3. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 86 al fine di precisare i criteri e i requisiti concernenti le misure e i meccanismi adeguati di cui ai paragrafi 1 e 2, in particolare i requisiti riguardanti la protezione dei dati fin dalla progettazione applicabili in materia trasversale a vari settori, prodotti e servizi. 4. La Commissione può stabilire norme tecniche riguardanti i requisiti di cui ai paragrafi 1 e 2. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 87, paragrafo 2".

NOTA 234 - Ai sensi dell'articolo 13 del "Codice in materia di protezione dei dati personali": "1. L'interessato o la persona presso la quale sono raccolti i dati personali sono

previamente informati oralmente o per iscritto circa: a) le finalità e le modalità del trattamento cui sono destinati i dati; b) la natura obbligatoria o facoltativa del conferimento dei dati; c) le conseguenze di un eventuale rifiuto di rispondere; d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi; e) i diritti di cui all'articolo 7; f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile. 2. L'informativa di cui al comma 1 contiene anche gli elementi previsti da specifiche disposizioni del presente codice e può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare in concreto l'espletamento, da parte di un soggetto pubblico, di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati. 3. Il Garante può individuare con proprio provvedimento modalità semplificate per l'informativa fornita in particolare da servizi telefonici di assistenza e informazione al pubblico. 4. Se i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione. 5. La disposizione di cui al comma 4 non si applica quando: a) i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria; b) i dati sono trattati ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento; c) l'informativa all'interessato comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile. 5-bis. L'informativa di cui al comma 1 non è dovuta in caso di ricezione di curricula spontaneamente trasmessi dagli interessati ai fini dell'eventuale instaurazione di un rapporto di lavoro. Al momento del primo contatto successivo all'invio del curriculum,

il titolare è tenuto a fornire all'interessato, anche oralmente, una informativa breve contenente almeno gli elementi di cui al comma 1, lettere a), d) ed f)".

NOTA 248 - L'articolo 7 del d.lgs. 196/2003, rubricato "diritto di accesso ai dati personali ed altri diritti", sancisce che: "1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile. 2. L'interessato ha diritto di ottenere l'indicazione: a) dell'origine dei dati personali; b) delle finalità e modalità del trattamento; c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2; e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati. 3. L'interessato ha diritto di ottenere: a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati; b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati; c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato. 4. L'interessato ha diritto di opporsi, in tutto o in parte: a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta; b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale".

NOTA 263 - L'articolo 17 del c.d. "Decreto del fare", rubricato "Misure per favorire la realizzazione del Fascicolo sanitario elettronico", sancisce: "1. All'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, sono apportate le seguenti modificazioni: a) al comma 2, dopo le parole: «Il FSE è istituito dalle regioni e province autonome,» sono inserite le seguenti: «conformemente a quanto disposto dai decreti di cui al comma 7, entro il 30 giugno 2015,»; b) dopo il comma 2, è inserito il seguente: «2-bis. Per favorire la qualità, il

monitoraggio, l'appropriatezza nella dispensazione dei medicinali e l'aderenza alla terapia ai fini della sicurezza del paziente, è istituito il dossier farmaceutico quale parte specifica del FSE, aggiornato a cura della farmacia che effettua la dispensazione»; c) al comma 6, le parole «senza l'utilizzo dei dati identificativi degli assistiti e dei documenti clinici presenti nel FSE» sono sostituite dalle seguenti «senza l'utilizzo dei dati identificativi degli assistiti presenti nel FSE»; d) al comma 7, le parole: «con decreto» sono sostituite dalle seguenti: «con uno o più decreti» e le parole: «i contenuti del FSE e» sono sostituite dalle seguenti: «i contenuti del FSE e del dossier farmaceutico nonchè»; e) al comma 15, dopo le parole: «dei servizi da queste erogate» sono aggiunte le seguenti: «, ovvero partecipare alla definizione, realizzazione ed utilizzo dell'infrastruttura nazionale per l'interoperabilità per il FSE conforme ai criteri stabiliti dai decreti di cui al comma 7, resa disponibile dall'Agenzia per l'Italia digitale,»; f) dopo il comma 15 sono aggiunti i seguenti commi: 15-bis. Entro il 30 giugno 2014, le regioni e le province autonome presentano all'Agenzia per l'Italia digitale e al Ministero della salute il piano di progetto per la realizzazione del FSE, redatto sulla base delle linee guida rese disponibili dalla medesima Agenzia e dal Ministero della salute, anche avvalendosi di enti pubblici di ricerca, entro il 31 marzo 2014. 15-ter. L'Agenzia per l'Italia digitale, sulla base delle esigenze avanzate dalle regioni e dalle province autonome, nell'ambito dei rispettivi piani, cura, in accordo con il Ministero della salute, con le regioni e le province autonome, la progettazione e la realizzazione dell'infrastruttura nazionale necessaria a garantire l'interoperabilità dei FSE. 15-quater. L'Agenzia per l'Italia digitale e il Ministero della salute operano congiuntamente, per le parti di rispettiva competenza, al fine di: a) valutare e approvare, entro sessanta giorni, i piani di progetto presentati dalle regioni e dalle province autonome per la realizzazione del FSE, verificandone la conformità a quanto stabilito dai decreti di cui al comma 7 ed in particolare condizionandone l'approvazione alla piena fruibilità dei dati regionali a livello nazionale, per indagini , valutazioni statistiche, registri nazionali e raccolta di dati a fini di programmazione sanitaria nazionale; b) monitorare la realizzazione del FSE, da parte delle regioni e delle province autonome, conformemente ai piani di progetto approvati. La realizzazione del FSE in conformità a quanto disposto dai decreti di cui al comma 7 è compresa tra gli adempimenti cui sono tenute le regioni e le province autonome per l'accesso al finanziamento integrativo a carico del Servizio sanitario nazionale da verificare da parte del Comitato di cui all'articolo 9 dell'intesa sancita il 23 marzo 2005 dalla Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano, pubblicata nel supplemento ordinario alla Gazzetta

Ufficiale n. 105 del 7 maggio 2005. 15-quinquies. Per il progetto FSE di cui al comma 15-ter, da realizzare entro il 31 dicembre 2015, è autorizzata una spesa non superiore ai 10 milioni di euro per l'anno 2014 e a 5 milioni di euro a decorrere dall'anno 2015, da definire su base annua con decreto del Ministero dell'economia e delle finanze su proposta dell'Agenzia per l'Italia digitale".

BIBLIOGRAFIA

ABDELHAK M., *Health Information Management of a Strategic Resource*, W. B. Saunders Company, Philadelphia, 1996

ALANAZI H. O., *Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance*, Journal of Medicinal Plants Research 2010, 4(19), pp. 2059-2074

ANDERSON J. G., *Security of the distributed electronic patient record: a case-based approach to identifying policy issues*, International Journal of Medical Informatics, 2000, 60, pp. 111-118

ANDERSON R. J., *Security in Clinical Information Systems*, University of Cambridge, 1996

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 08/2012 providing further input on the data protection reform discussions*, WP199, 01574/12/EN, Brussel, 2012

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 15/2011 on the definition of consent*, adopted on 13 July, 201101197/11/EN, WP187

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Working Document on the processing of personal data relating to health in electronic health records (EHR)*, adopted on 15 February 2007, 00323/07/EN, WP 131

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Thirteenth Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and in third countries covering the year 2009*, adopted on 14 July 2010, Brussels, 2011

ARTICOLO 29 GRUPPO DI LAVORO PER LA PROTEZIONE DEI DATI PERSONALI, *Parere 4/2007 sul concetto di dati personali*, adottato il 20 giugno, 01248/07/IT, WP 136

ATIENZA A. ET AL., *Critical Issues in eHealth Research*, Am J Prev Med, 2007, 32 pp. 5-ss.

BAKER G.R., NORTON P., *Patient Safety and Healthcare Error in the Canadian Healthcare System. A Systematic Review and Analysis of Leading Practices on Canada with Reference to Key Initiatives Elsewhere. A Report to Health Canada*, Ottawa, Health Canada, 2002

BARRY R. ET AL., *Hype Cycle for Healthcare Provider Applications and Systems*, Report number G00127849, Stamford CT: Gartner Research, 2005

BASSI E., *PSI, protezione dei dati personali, anonimizzazione*, in "Informatica e diritto", ESI Italiane, Napoli, fasc. 1-2, 2011, pp. 65-84

BATES D.W. ET AL., *The impact of computerized physician order entry on medication error prevention*, Journal of the American Medical Informatics Association", 1999, 6(4), pp. 313-321

BERNSTEIN K. ET AL., *Modelling and implementing electronic health records in Denmark*, International Journal of Medical Informatics, 2005, 74, pp. 213-220

BILLON M. ET AL., *Disparities in ICT adoption: A multidimensional approach to study the cross-country digital divide*, Telecommunications Policy, 2009, 33, pp. 596–610

BIRNHACK M. D., *The EU Data Protection Directive: An engine of a global regime*, Computer Law&Security Report, 2008, 24, pp. 508-520.

BJERKNES, G., BRATTETEIG T., *Florence in Wonderland. System Development with Nurses*, in Bjerknes G., Ehn P., and Kyng M. (eds.), "Computers and Democracy. A Scandinavian Challenge", Aldershot, UK: Avebury, 1987

BJERKNES, G., BRATTETEIG T., *User Participation and Democracy: A Discussion of Scandinavian research on System Development*, Scandinavian Journal of Information Systems, 1995, 1, pp. 73-98

BLOBEL B., PHAROW P., *Analysys and Evaluation of EHR Architecture*, Method Inf. Med., 2009, 2, pp. 162-169.

BØDKER K. ET AL., *Participatory IT design: Designing for business and workplace realities*, Cambridge, MA: MIT Press, 2004

BORKING J., RAAB C., *Laws, PETs and Other Technologies for Privacy Protection*, The Journal of Information, Law and Technology, 2001, 1

BOS' J.J., *Digital signatures and the electronic health records: providing legal and security guarantees*, International Journal of Bio-Medical Computing, 1996, 42, pp. 157-163

BROWN N., REYNOLDS M., *Strategy for production and maintenance of standards for interoperability within and between service departments and other healthcare domains*, Short Strategic Study CEN/TC251/N00-047, CEN/TC 251 Health Informatics, Brussels, Belgium, 2000

BUSCEMI A., CARRARO A., *L'innovazione tecnologica RFID a garanzia della sicurezza del paziente*, in "Diritto Sanitario Moderno", 2011, 59, pp. 1-12

CANNON D.S., ALLEN S.N., *A comparison of the effects of computer and manual reminders on compliance with a mental health clinical practice guideline*, Journal of American Medical Information Association, 2000, 7, pp. 196-203

CARVALHO D.ET AL., *New interaction paradigms to fight the digital divide: a pilot case study regarding multi-touch technology*, Procedia Computer Science, 2012, 14, pp. 128-137

CAVOUKIAN A. (presentation by), *Privacy by Design: Building Trust into Technology*, 1st Annual Privacy and Security Workshop. Centre for Applied Cryptographic Research, Toronto, 2000

CAVOUKIAN A., ALVAREZ R. C., *Embedding Privacy into the Design of EHRs to Enable Multiple Functionalities - Win/Win*, Toronto, 2012, pp. 19

CAVOUKIAN A., CHANLIAU M., *Privacy and Security by Design: A Convergence of Paradigms*, Toronto, 2013, pp. 19

CAVOUKIAN A., EL EMAM K., *A Positive-Sum Paradigm in Action in the Health Sector*, Toronto, 2010, pp. 6

CAVOUKIAN A., *Moving Forward From PETs to PETs Plus: The Time for Change is Now*, Toronto, 2009, pp. 4

CAVOUKIAN A., *Privacy by Design … Take the Challenge*, Toronto, 2009, pp. 361

CAVOUKIAN A., *Privacy by Design. The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices*, Toronto, 2010, pp. 12

CAVOUKIAN A., *Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era*, in Yee G.O.M., Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards, IGI Global, Hershey, 2012, pp. 170-208

CHING HSU I., *Extensible access control markup language integrated with Semantic Web technologies*, Information Sciences, 2013

CLAERHOUTA B., DEMOORB G.J.E., *Privacy protection for clinical and genomic data: The use of privacy-enhancing techniques in medicine*, International Journal of Medical Informatics, 2005, 74, 2-4, pp. 257-265

CODAGNONE C., LUPIÁÑEZ-VILLANUEVA F., *A composite index for the benchmarking of eHealth Deployment in European acute Hospitals. Distilling reality in manageable form for evidence based policy*, JRC Technical and Scientific Reports, Luxembourg: Publication Office of the European Union, 2011

COLLINGRIDGE D., *The Social Control of Technology*, St. Martin's Press, Frances Pinter, 1980

COMMISSIONE DI COORDINAMENTO SPC (SISTEMA PUBBLICO DI CONNETTIVITÀ E COOPERAZIONE), *Linee guida per l'interoperabilità semantica attraverso i Linked Open Data*, v. 1.3, 2012, pp. 102

CONKLIN WM. A., WHITE G., *Principles of Computer Security. CompTIA Security+TM and Beyond*, The United States of America, Mc Graw Hill, Second edition

CORASANITI G., *La sicurezza dei dati personali*, in Cardarelli, Sica, Zeno-Zencovich (a cura di), "Il codice dei dati personali. Temi e problemi", Giuffrè, Milano, 2004, pp. 112-163

CORDASEV H. ET AL., *Cross border care EU: How to choose the best hospital? A study of hospital information portals in five EU countries*, Health Consumer Powerhouse, Danderyd, Sweden/Brussels, 2010

CRUZ-JESUS F. ET AL., *Digital divide across the European Union*, Information & Management, 2012, 49, pp. 278-291

CURRIE W. L., *Towards a Healthier Europe!*, The TEMPEST Model, 2010

D'AGOSTINI D. ET AL., *La sicurezza delle informazioni in ambito sanitario*, in "Mondo Digitale", 2010, 2, pp. 59-66

DANZON P.M., FURUKAWA M., *e-Health: Effects of the Internet on Competition and Productivity in Health Care*, in Rivlin A. M., Liton R. E. (eds.), "The Economic Payoff from the Internet Revolution", Washington DC, The Brookings Task Force on the Internet, Brookings Institution Press, 2001

DEKKER M.A.C., ETALLE S., *Audit-Based Access Control for Electronic Health Records*, Electronic Notes in Theoretical Computer Science, 2007, 168, pp. 221–236

DI COCCO C., *Soggetti che effettuano il trattamento (Parte I-Titolo IV)*, in J. Monducci, G. Sartor, "Il codice in materia di protezione dei dati personali", CEDAM, Padova, 2004, pp. 119-156

DICK R., STEEN E. B., DETMER D. (eds.), *The Computer Based Patient Record: An Essential Technology for Health Care*, Institute of Medicine, National Academy Press, 1997, p. 111

DOBREV A. ET AL., *Interoperable eHealth is Worth it. Securing Benefits from Electronic Health Records and ePrescribing. Study Report 2010*, European Communities, Bonn/Brussels, 2010, pp. 88

DOBREV A. ET AL., *Report on The socio-economic impact of interoperable electronic health record (EHR) and ePrescribing systems in Europe and beyond. Final study report, Deliverable D3.4 of the EHR IMPACT study*, 2009, pp. 54

DOBREV A. ET AL., *Benchmarking ICT use among General Practitioners in Europe*, Final Report . Brussels/Bonn, 2008

DOLIN R.H. ET AL., *HL7 Clinical Document Architecture, Release 2*, J Am Med Inform Assoc., 2006, 13(1), pp. 30-39

DUGAS M. ET AL., *Benchmarking of hospital information systems: Monitoring of discharge letters and scheduling can reveal heterogeneities and time trends*, BMC Medical Informatics and Decision Making. 2008, 8 pp. 15 ss.

E-BUSINESS W@TCH,. *ICT and e-business in Hospital Activities. ICT and e-business activity in 2006*, Sector Report No. 10 2006, Bonn: Empirica; Brussels: European Commission, 2006

EHEALTH ERA, *eHealth priorities and strategies in European countries. Towards the Establishment of a European eHealth Research Area*, Brussel, 2007, pp. 100

EHEALTH TASK FORCE, *Redesigning health in Europe for 2020*, Luxemburg, 2012, pp. 12

EICHELBERG M. ET AL., *Electronic Health Record Standards - a brief overview, conference paper for Information Processing in the Service of Mankind and Health*, ITI 4th International Conference on Information and Communications Technology, 2006

EL EMAM K. ET AL., *De-identification methods for open health data: the case of the Heritage Health Prize claims dataset*, J Med Internet Res., 2012, Feb 27; 14(1):e33.

EMPIRICA & WRC [WORK RESEARCH CENTRE], *ICT & Ageing – European study on Users, Markets and Technologies, Preliminary findings*, Interim report, Bonn: Empirica; Dublin: Work Research Centre, 2008

EMPIRICA, *European countries on their journey towards national eHealth infrastructures*, eHealth Strategies Report, 2011, pp. 47

EMPIRICA, *ICT standards in the health sector: current situation and prospects*, Final report, v. 3.0, Special Study n. 1, 2008, pp. 84

ERA, *eHealth strategies and implementation in European countries*, EHealth ERA Report, Luxembourg, Office for Official Publications of the European Communities, 2007,pp. 100

EUROPEAN COMMISSION, *Explanatory Memorandum, Scope of the Recommendation*, Draft Commission Recommendation of 2nd July 2008 on cross-border interoperability of electronic health record systems, Brussels: European Commission, 2008

EUROPEAN COMMISSION, *Connected Health - Quality and Safety for European Citizens*, Report of the Unit ICT for Health in collaboration with the i20 sub-group on e-health and the eHealth stakeholders' group, 2006

EUROPEAN COMMISSION, *ICT for Health & i2010 - Transforming the European healthcare landscape – Towards a strategy for ICT for Health*, 2006

EUROPEAN COMMISSION, *Accelerating the Development of the eHealth Market in Europe*, Brussel, 2007, pp. 36

EUROPEAN COMMISSION, *eHealth for Safety. Impact of ICT on Patient Safety and Risk Management*, Belgium, 2007, pp. 70

EUROPEAN COMMISSION - DIRECTORATE-GENERAL JUSTICE, FREEDOM AND SECURITY, *Comparative Study On Different Approaches To New Privacy Challenges, In Particular In The Light Of Technological Developments*, Final Report, Centre for Public Reform, Final version, 2010, pp. 59

EUROPEAN COMMISSION, *European Interoperability Framework for Pan-European egovernment Services*, Luxemburg, 2004, pp. 26

EUROPEAN COMMISSION, *M/403 Mandate to the European Standardisation Organisations CEN, CENCELEC and ETSI in the Field of Information and Communication Technologies, Applied to the Domain of eHealth*, 2006

EUROPEAN COMMISSION, *Unlocking the ICT growth potential in Europe: Enabling people and businesses*, Luxemburg, 2014

EUROPEAN COMMISSION, *eHealth priorities and strategies in European countries*, eHealth ERA report, Brussels, 2007

EUROPEAN COMMITTEE FOR STANDARDIZATION, *Information Society Standardisation System eHealth Standardisation Focus Group*, 2005

EUROPEAN COMMISSION, *Accelerating the Development of the eHealth Market in Europe*, eHealth Taskforce Report, Luxembourg, Office of Official Publications of the European Communities, 2007

EUROPEAN COMMISSION, *Interoperable eHealth is worth it. Securing benefits from eRecords and ePrescribing*, Luxembourg, Office of Official Publications of the European Communities, 2010

EUROPEAN COUNCIL, *Council Conclusions on Common values and principles in European Union Health Systems*, Document 2006/C 146/01, The Official Journal of the European Union, 2006

EUROPEAN PARLIAMENT, *European Parliament legislative resolution of 19 January 2011 on the Council at first reading with a view to the adoption of a directive of the European Parliament and of the Council on the application of patients' rights in cross-border healthcare*, 2011

EUROSTAT, *Health statistics: Key data on health 2002. Data 1970-2001*, Luxembourg: Office of Official Publications of the European Communities, 2002

EYSENBACH G., *What is e-health?*, Journal of Medical Internet Research, 2001, 3(2):e20

FERNÁNDEZ-ALEMÁN J. L. ET AL., *Security and privacy in electronic health records: A systematic literature review*, Journal of Biomedical Informatics, 2013

FERRAIOLO D. F., KUHN D. R., *Role-Based Access Controls*, 15th National Computer Security Conference, Baltimore MD, 1992, pp. 554-563

FINOCCHIARO G., *voce Anonimato*, in Basile, Sacco, Scala (con la collaborazione di), "Digesto delle discipline privatistiche", Iannarelli-Rook, sez. civ., agg., Torino, 2010

FLATLEY BRENNAN P. ET AL., *Project HealthDesign: Rethinking the power and potential of personal health records*, Journal of Biomedical Informatics, 2010, 43, S3-S5

FLORIO A., *Il trattamento dei "dati idonei a rivelare lo stato di salute" da parte dei medici liberi professionisti*, in "Ciberspazio e Diritto", 2010, vol. 11, n. 1, pp. 111-145

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Autorizzazione al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale*, Autorizzazione n. 2/2013, pubblicata in G.U. n. 302 del 27.12.2013, valida dal 1° gennaio 2014 al 31 dicembre 2014, salve eventuali modifiche del Garante

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Relazione 2010. Evoluzione tecnologica e protezione dei dati*, 2010, pp. 320

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Trattamento di dati personali contenuti nel Registro Italiano di Dialisi e Trapianto*, 16 gennaio 2014, Registro dei provvedimenti n. 16 del 16 gennaio 2014

GARETS D., DAVIS M., *Electronic Patient Records. EMRs and EHRs*, Healthcare Informatics, 2005

GARTNER, *eHealth for a Healthier Europe! – opportunities for a better use of healthcare resources*, Västerås, Sweden: Edita, 2009

GOLDBERG I. ET AL., *Privacy-Enhancing Technologies for the Internet*, in "Proceedings of IEEE COMPCON '97", 1997, pp. 103-109

GRITZALISA D., LAMBRINOUDAKIS C., *A security architecture for interconnecting health information systems*, International Journal of Medical Informatics, 2004, 73, pp. 305-309

GROENE O. ET AL., *Investigating organizational quality improvement systems, patient empowerment, organizational culture, professional involvement and the quality of care in European hospitals: the 'Deepening our Understanding of Quality Improvement in Europe (DUQuE)' project*, British Medical Council Health Services Research, 2010, 10, pp. 281

GRÜN O., *Taming Giant Projects. Management of Multi-Organization Enterprises*, Berlin, Springer, 2004, pp. 271

GÜRSES S. ET AL., *Engineering Privacy by Design*, in "Conference of Computers, Privacy & Data Protection", 2011, pp. 25

GUY P. ET AL., *Systematic Review of Home Telemonitoring for Chronic Diseases: The Evidence Base*, Journal of the American Medical Informatics Association, 2007, 14(3), pp. 269-277

HAAS S. ET AL., *Aspect of privacy for electronic health records*, International Journal of Medical Informatics, 2011, 80, e26-e31

HAWN C., *Take Two Aspirin and Tweet Me in the Morning: How Twitter, Facebook, and Other Social Media are Reshaping Healthcare*, Health Affairs, 2009, 28 (2), pp. 361-365

HÄYRINEN K. ET AL., *Definition, structure, content, use and impacts of electronic health records: A review of the research literature*, International Journal of Medical Informatics, vol. 77, 2008, pp. 291-304

HEATH T., BIZER C., *Linked Data: Evolving the Web into a Global Data Space*, 1st edition, Synthesis Lectures on the Semantic Web: Theory and Technology, Morgan & Claypool, 2012, 1:1, pp. 1-136

HILLESTAD R. ET AL., *Can electronic medical record systems transform healthcare? Potential health benefits, savings, and costs*, Health Affairs, 2005, 24(5), pp.1103-1117

HOERBST A., AMMENWERTH E., *Quality and Certification of Electronic Health Records. An overview of current approaches from the US and Europe*, Applied Clinical Informatics, 2010, pp. 149-164

HOLZINGER A. ET AL., *Ubiquitous Computing for Hospital Applications: RFID-Applications to Enable Research in Real-Life Environments*, in "29th Annual International Computer Software and Applications Conference (COMPSAC'05)", 2005, vol. 2, pp. 19-20

HUANG L. ET AL., *Privacy preservation and information security protection for patients' portable electronic health records*, Computers in Biology and Medicine, 2009, 39, pp. 743-750

HÜBNER U. ET AL., *ICT supporting nurses and physicians in hospitals: results of a comparative survey in Austria and Germany*, Studies in Health Technology and Informatics, 2009; 146:20-4

HÜBNER U. ET AL., *IT adoption of clinical information systems in Austrian and German hospitals: results of a comparative survey with a focus on nursing*, BMC Medical Informatics and Decision Making, 2010, 10:8

IAKOVIDIS I., *Towards Personal Health Record: Current situation, obstacles and trends in implementation of Electronic Healthcare Records in Europe*, International Journal of Medical Informatics, 1998, 52, 128, pp. 105-117

IDABC, EIF, *European Interoperability Framework for Pan-european eGovernment Services*, v. 1.0, Brussel, 2004, pp. 25

INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, DUTCH REGISTRATIERKAMER, *Privacy Enhancing Technologies - The Path to Anonymity*, Registratiekamer, The Netherlands, Voll. I-II, 1995

IZZO U., GUARDA P., *Sanità elettronica, tutela dei dati personali e digital divide generazionale. Ruolo e criticità giuridica della delega alla gestione dei servizi di sanità elettronica da parte dell'interessato*, Trento Law and Technology Research Group, Research Paper Series n. 3, 2010,

KARLA D., *Electronic Health Records Standards*, IMIA Year Book of Medical Informatics, 2006, pp. 136-144

KAZLEY A.S., OZCAN Y.A., *Organizational and environmental determinants of hospital EMR adoption: a national study*, Journal of medical systems, 2007, 31(5), pp. 375-84

KHARRAZI H. ET AL., *Mobile personal health records: An evaluation of features and functionality*, International Journal of Medical Informatics, Vol. 81, Issue 9, 2012, pp. 579-593

KREIZMAN G., ROBERTSON B., Incorporating Security into the Enterprise Architecture Process, Gartner, 2006

KREPS G. L., NEUHAUSER L., *New directions in eHealth communication: Opportunities and challenges*, Patient Education and Counseling, 2010, 78, pp. 329-336

KUM H.C., AHALT S., *Privacy-by-Design: Understanding Data Access Models for Secondary Data*, AMIA Summits Transl Sci Proc., 2013, pp. 126-30

LE XUAN H. ET AL., *Activity-oriented access control to ubiquitous hospital information and services*, Information Sciences, 2010, 180, pp. 2979-2990

LONDON ECONOMICS, *Study on the economic benefits of privacy-enhancing technologies (PETs)*, Final Report to The European Commission DG Justice, Freedom and Security, London, 2010, pp. 238

MALIN B. AT AL., *Biomedical data privacy: problems, perspectives, and recent advances*, J Am Med Inform Assoc, 2013, 20, pp. 2-6

MALIN B. ET AL., *Technical and policy approaches to balancing patient privacy and data sharing in clinical and translational research*, J Investig Med., 2010, 58(1), pp. 11-8

MALIN B., ET AL., *Learning relational policies from electronic health record access logs*, Journal of Biomedical Informatics, 2011, 44, pp. 333–342

MARTIN D., SERJANTOV A. (edited by), *Privacy Enhancing Technologies, Proceeding of 4° international workshop PET 2004*, Toronto - Berlin, 2004

MINISTERO DELLA SALUTE, *Il Fascicolo Sanitario Elettronico. Linee guida nazionali*, Roma, 2010, pp. 28

MOEREL L., *Big Data Protection. How to Make the Draft EU Regulation on Data Protection Future Proof*, Tilburg University, 2014, pp. 68

MORUZZI M., *e-Health e Fascicolo Sanitario Elettronico*, Il Sole 24 Ore, 2009, pp. 364

NATIONAL INSTITUTES OF HEALTH - NATIONAL CENTER FOR RESEARCH RESOURCES, *Electronic Health Record Overview*, MITRE Center for Enterprise, McLean, Virginia, 2006, pp. 30

NORDIC COUNCIL OF MINISTERS, *Health and Social Sectors with an "e". A study of the Nordic countries*, 2005, Copenhagen, pp. 165

NORRIS P., *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide*, Cambridge University Press, Oxford, 2001, pp. 3 e ss.

OECD HEALTH POLICY STUDIES, *Improving Health Sector Efficiency. The Role of Information and Communication Technologies*, 2010

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, *7 Essential Steps for Designing Privacy into Technology*, Toronto, 2002

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, *Privacy Protection Makes Good Business Sense*, Toronto, 1994

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, *Privacy: The Key to Electronic Commerce*, Toronto, 1998

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, REGISTRATIERKAMER THE NETHERLANDS, *Intelligent Software Agents: Turning a Privacy Threat into a Privacy Protector. Result of a joint project of the Office of the Information and Privacy Commissioner/Ontario and the Registratierkamer*, The Netherlands, 1999

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, Smart, *Optical and Other Advanced Cards: How to Do a Privacy Assessment*, Toronto, 1997

OH H. ET AL., *What Is eHealth: A Systematic Review of Published Definitions*, Journal of Medical Internet Research, 2005, 7(1), e1

OPEN DEFINITION, *Defining the Open in Open Data, Open Content and Open Services*, 2012

OPEN KNOWLEDGE FOUNDATION, *Open Data Handbook Documentation*, Rel. 1.0.0, 2012, pp. 23

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY - COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY, WORKING PARTY ON INFORMATION SECURITY AND PRIVACY, *Inventory of Privacy-Enhancing Technologies (PETs)*, DSTI/ICCP/REG(2001)1/FINAL, 2002, pp. 29

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, *Improving Health Sector Efficiency: The Role of Information and Communication Technologies*, OECD Health Policy Studies. Paris: OECD Publishing, 2010

PAGALLO U., BASSI E., *The Future of EU Working Parties' "The Future of Privacy" and the Principle of Privacy by Design*, in M. Bottis (eds.), "An Information Law for the 21st Century", Atene, Nomiki Bibliothiki, 2011, pp. 286-305

PAGALLO U., *Designing Data Protection Safeguards Ethically*, in Information, 2011, 2, pp. 247-265

PAGALLO U., *On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law*, in S. Gutwirth et al. (eds.), "European Data Protection: In Good Health?", Springer Science+Business Media B.V, 2012, pp. 331-346

PAGALLO U., *Privacy e Design*, in M. Pietrangelo (a cura di), "Diritti di libertà nel mondo virtuale della rete", Informatica e diritto, 2009, 1, pp. 123-134

PAGLIARI C. ET AL., *Potential of electronic personal health records*, British Medical Journal, 2007, pp. 330-333

PATHAK J. ET AL., *Applying linked data principles to represent patient's electronic health records at Mayo clinic: a case report*, in "Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium", ACM New York, USA, 2012, pp. 455-464

PERRI P., *Introduzione alla sicurezza informatica e giuridica*, in Pattaro E. (a cura di), "Manuale di diritto dell'informatica e delle nuove tecnologie", Clueb s.c.a.r.l., Bologna, 2002, pp. 306 e ss.

PERRI P., *Le misure di sicurezza*, in Monducci J., Sartor G., "Il codice in materia di protezione dei dati personali", CEDAM, Padova, 2004, pp. 137 e ss.

PERRI P., *Privacy, diritto e sicurezza informatica*, Giuffrè, Milano, 2007, pp. 195

PHILIPP A. ET. AL., *Hacking Exposed: Computer Forensics*, second edition, McGraw Hill, 2009, pp. 544

PINO G., *Teorie e dottrine dei diritti della personalità Uno studio di meta-giurisprudenza analitica*, in "Materiali per una storia della cultura giuridica", Bologna, Il Mulino, 2003, 1, pp. 237-274

Q-REC, WP3, *Inventory of Relevant Standards for EHR Systems*, v. 0.8, 2007, pp. 95

RABAZZI C. ET AL., *La sicurezza informatica e la Privacy*, in G. Ziccardi (a cura di), "Telematica giuridica. Utilizzo avanzato delle nuove tecnologie da parte del professionista del diritto", Giuffrè, Milano, 2005, pp. 516 e ss.

RABBITO C., *Sanità elettronica e diritto. Problemi e prospettive*, Società Editrice Universo, 2010, pp. 118

REIMER S., *Current and Future Settings of Austrian Legislation Regarding Electronic Health Records (EHR)*, EJBI, 2012, 8 (2), pp. 11-28

RODOTÀ S., *Privacy e costruzione della sfera privata (1991)*, in Id., "Tecnologie e diritti", Bologna, Il Mulino, 1995, pp. 101-122.

ROSENTHAL J., RILEY T., *Patient safety and medical errors: a roadmap for state action*, National Academy for State Health Policy, 2001

ROSSI MORI A. ET AL. (a cura di), *Un quadro di riferimento sulle tecnologie dell'informazione nel settore sanitario*, Consiglio Nazionale delle Ricerche - Istituto Tecnologie Biomediche, 2003, pp. 64

ROVATI A. M., *Prime note su proprietà intellettuale e riutilizzo dei dati pubblici*, in Informatica e diritto, ESI, Napoli, fasc. 1-2, 2011, pp. 153-184

SADAN B., *Patient data confidentiality and patient rights*, International Journal of Medical Informatics, 2001, 62, pp. 41–49

SANDHU R. ET AL., *The NIST Model for Role-Based Access Control: Towards A Unified Standard*, Proceedings of the fifth ACM workshop on Role-based access control, 2000, pp. 46-63

SANDHU R. S. ET AL., *Role-Based Access Control Models*, IEEE Computer, 1996, 29 (2), pp. 38-47

SAPPA C., *Diritti di proprietà intellettuale e dati pubblici nell'ordinamento italiano*, in Informatica e diritto, ESI, Napoli, fasc. 1-2, 2011, pp. 185-198

SCHAAR P., *Privacy by Design*, Identity in Information Society, 2010, 3, pp. 267-274

SITTIG D. F., *Personal health records on the internet: a snapshot of the pioneers at the end of the 20th Century*, International Journal of Medical Informatics, 2002, 65, 1–6

SMITH E., ELOFF J.H.P., *Security in health-care information systems-current trends*, International Journal of Medical Informatics, 1999, 54, pp. 39-54

STRANDBERG M., KRASNIK A., *Does a public single payer system deliver integrated care? A national survey among professional stakeholders in Denmark*, International Journal of Integrated Care, 2008.

STROETMANN K. A. ET AL., *eHealth is worth it. The economic benefits of implemented eHealth solutions at ten European sites*, Luxembourg, Office of Official Publications of the European Communities, 2006

STROETMANN K. A. ET AL., *eHealth in Action. Good Practice in European Countries. Good eHealth Report*, Luxemburg, 2009, pp. 60

STROETMANN K. A. ET AL., *European countries on their journey towards national eHealth infrastructures. eHealth Strategies Report*, Bruxelles, 2011, pp. 61

STROETMANN K. A., STROETMANN V. N., *Electronic business in the health and social services sector*, Sector Impact Study No. 10-I (draft), The European e-business W@tch 2003/4, Commissione europea, Direzione generale Imprese: Bruxelles/Bonn, 2004

SUMMERFIELD B., EMPEY E., *Computer-based Information Systems for Medicine: A Survey and Brief Discussion of Current Projects*, Santa Monica, Calif.: Systems Development Corporation, 1965

SUOMINEN H., *Towards an international electronic repository and virtual laboratory of open data and open-source software for telehealth research: comparison of international, Australian and Finnish privacy policies*, Stud Health Technol Inform., 2012, 182, pp. 153-60

T. BERNERS-LEE, *Is your Linked Open Data 5 Star?*, 2009

TANG P. C., ET AL., *Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption*, Journal of the American Medical Informatics Association, 2006, 13 (2), pp. 121-126

TETTERO O., *Intrinsic Information Security: Embedding Security Issues in the Design Process of Telematics Systems*, Technical Report 6, Telematica Instituut, Enschede, The Netherlands, 2000

THE DEPARTMENT FOR CULTURE, MEDIA AND SPORT AND THE DEPARTMENT FOR BUSINESS, INNOVATION AND SKILLS, *Digital Britain*, Final Report, 2009, London, The Stationery Office, pp. 238

THURAISINGHAM B., *Security standards for the semantic web*, Computer Standards & Interfaces, 2005, 27, pp. 257-268

TSAI C., STARREN J., *Patient Participation in Electronic Medical Records*, Journal of the American Medical Association, 2001, 285 (13), p. 1765

UECKERT F. ET AL., *Empowerment of patients and communication with health care professionals through an electronic health record*, International Journal of Medical Informatics, 2003 70 (2-3), pp. 99-108

VAN BLARKOM RE G.W., BORKING J.J., OLK J.G.E. (eds.), *Handbook of Privacy and Privacy-Enhancing Technologies. The case of Intelligent Software Agents*, PISA Consortium, The Hague, 2003, pp. 372

VAN DER SLOOT B., *Public Sector Information & Data Protection: A Plea for Personal Privacy Settings for the Re-use of PSI*, in "Informatica e diritto", ESI, Napoli, fasc. 1-2, 2011, pp. 219-238

VAN DEURSEN A. J.A.M., *Internet skill-related problems in accessing online health information*, International Journal of Medical Informatics, 2012, 81, pp. 61-72

VICENTE M. R., LÓPEZ A. J., *Assessing the regional digital divide across the European Union-27*, Telecommunications Policy, 2011, 35, pp. 220-237

VIOLA DE AZEVEDO M. ET AL., *La re-identificazione dei dati anonimi e il trattamento dei dati personali per ulteriore finalità: sfide alla privacy*, Ciberspazio e diritto 2010, 11, pp. 641-655

WAEGEMANN P., *Status Report 2002: Electronic Health Records*, Medical Records Institute, 2002

WARREN S., BRANDEIS L., *The Right to Privacy*, in Harvard Law Review, 1890, 4, pp. 193-220

WESTIN A., *Privacy and Freedom*, Bodley Head, 1967, pp. 487

WILSON P. ET AL., *Mapping the Potential of eHealth. Empowering the citizen through eHealth tools and services*, Maastricht, European Institute of Public Administration2004,

WORLD HEALTH ORGANISATION. *Telemedicine: Opportunities and developments in Member States. Based on the findings of the second global survey on eHealth*, Global observatory for eHealth series - Vol 2, Geneva, WHO Press, 2010

WORLD HEALTH ORGANISATION, *ATLAS. eHealth country profiles. Based on the findings of the second global survey on eHealth*, Global observatory for eHealth series – Vol. 1, Geneva, WHO Press, 2011

WORLD HEALTH ORGANISATION, *Cross-border Health Care in the European Union. Mapping and analysing practices and policies*, Observatory Studies Series 22, 2011, pp. 395

WORLD HEALTH ORGANISATION, *mHealth: New Horizons for Health through Mobile Technologies, Global Observatory for eHealth Services*, Global observatory for eHealth series - Vol. 3, 2011

WORLD HEALTH ORGANISATION, *eHealth. TOOLS&SERVICES. Needs of the Member States. Report of the WHO Global Observatory for eHealth*, Switzerland, 2006, pp. 30

SELEZIONATI PROVVEDIMENTI LEGISLATIVI ITALIANI CITATI

d. lgs. 30 giugno 2003 n. 196, *Codice in materia di protezione dei dati personali*, pubblicato in G.U. n. 174 del 29.07.2003 e successive modifiche

d. lgs. 28 febbraio 2005 n. 42, *Istituzione del sistema pubblico di connettività e della rete internazionale della pubblica amministrazione, a norma dell'articolo 10, della legge 29 luglio 2003*, n. 229, pubblicato in G.U. n. 73 del 30.3.2005.

d.lgs. 7 marzo 2005 n. 82, *Codice dell'amministrazione digitale*, pubblicato in G.U. n.112 del 16.05.2005 e successive modifiche

d.lgs. 24 gennaio 2006 n. 36, *Attuazione della direttiva 2003/98/CE relativa al riutilizzo di documenti nel settore pubblico*, pubblicato in GU. n. 37 del 14.02.2006

d.lgs. 150/2009, *Attuazione della legge 4 marzo 2009 n. 15, in materia di ottimizzazione della produttività del lavoro pubblico e di efficienza e trasparenza delle pubbliche amministrazioni*, pubblicato in G.U. n. 254 del 31.10.2009

d.L. 9 febbraio 2012 n. 5, *Disposizioni urgenti in materia di semplificazione e di sviluppo*, pubblicato in G.U. n. 33 del 09.02.2012, convertito con modificazioni dalla legge 4 aprile 2012 n. 35

d.L. 13 settembre 2012 n. 158, *Disposizioni urgenti per promuovere lo sviluppo del Paese mediante un più alto livello di tutela della salute*, pubblicato in G.U. 13.11.2012 n. 214 e coordinato con legge di conversione 8 novembre 2012 n. 189

d.L. 18 ottobre 2012 n. 179, *Ulteriori misure urgenti per la crescita del Paese*, pubblicato in G.U. n. 245 del 19.10.2012

d.L. 22 giugno 2012 n. 83, *Decreto Sviluppo*, pubblicato in G.U. n. 147 del 26.6.2012, convertito, con modificazioni, dalla legge 7 agosto 2012 n. 134, pubblicata in G.U. n. 187 del 11.8.2012

d.L. 21 giugno 2013 n. 69, *Disposizioni urgenti per il rilancio dell'economia*, coordinato con legge di conversione 9 agosto 2013 n. 98, pubblicato in G.U. n. 144 del 21.06.2013

L. 31 dicembre 1996 n. 675, *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*, pubblicata in G.U. n. 5 del 8.1.1997

L. 18 giugno 2009 n. 69, *Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile*, pubblicato in G.U. n. 140 del 19.06.2009

L. 17 dicembre 2012 n. 221, *Conversione in legge, con modificazioni, del decreto-legge 18 ottobre 2012, n. 179, recante ulteriori misure urgenti per la crescita del Paese*, pubblicata in G.U. n. 294 del 18.12.2012

SELEZIONATI PROVVEDIMENTI COMUNITARI CITATI

Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati

Directive 97/7/EC of 20 May 1997 on the protection of consumers in respect of distance contracts

Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data, and the protection of privacy in the telecommunications sector

Direttiva 98/34/CE del Parlamento europeo e del Consiglio del 22 giugno 1998 che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

EC Regulation No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data

Directive 2001/83/EC of the European Parliament and of the Council of 2 November 2001 on the Community code relating to medicinal products for human use

Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati, pubblicato in G.U. L 008 del 12.01.2001

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

Direttiva 2003/98/CE del Parlamento europeo e del Consiglio del 17 novembre 2003 relativa al riutilizzo dell'informazione del settore pubblico, così come modificata dalla Direttiva 2013/37/UE del Parlamento europeo e del Consiglio del 26 giugno 2013

COMMISSIONE DELLE COMUNITÀ EUROPEE, *Prima relazione sull'applicazione della direttiva sulla tutela dei dati (95/46/EC)*, COM(2003) 265 def.

CEC, *Follow-up to the high level reflection process on patient mobility and health care developments in the European Union*, COM(204) 301 final, Brussels, 20.04.2004

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, *e-Health - making healthcare better for European citizens: An action plan for a European e-Health Area*, COM(2004)356 final

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, *i2010 - A European Information Society for growth and employment*, COM(2005)229 final

Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market

COMUNICAZIONE DELLA COMMISSIONE AL CONSIGLIO, AL PARLAMENTO EUROPEO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI, *Una strategia per una società dell'informazione sicura - Dialogo, partenariato e responsabilizzazione*, Bruxelles, 31.5.2006, COM(2006)251 def.

COMMISSIONE DELLE COMUNITÀ EUROPEE, *Comunicazione della Commissione al Parlamento europeo e al Consiglio sulla promozione della protezione dei dati mediante tecnologie di rafforzamento della tutela della vita privata (PET), Bruxelles*, COM(2007) 228 def.

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, *A Lead Market Initiative for Europe*, COM(2007)860 final

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS *on telemedicine for the benefit of patients, healthcare systems and society*, COM(2008)689 final

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, *Telemedicine for the benefit of patients, healthcare systems and society*, COM(2008)689 final

Commission Recommendation of 2nd July 2008 on cross-border interoperability of electronic health record systems, COM(2008)3282 final

COMMISSIONE DELLE COMUNITÀ EUROPEE, *Raccomandazione della Commissione del 2 luglio 2008 sull'interoperabilità transfrontaliera dei sistemi di cartelle cliniche elettroniche* [notificata con il numero C(2008) 3282] (2008/594/CE), pubblicata in GUCE L 190/37 del 18.7.2008

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI, *Riutilizzo dell'informazione del settore pubblico - Riesame della direttiva 2003/98/CE* -, COM(2009) 212 def.

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, *Solidarity in health: Reducing health inequalities in the EU*, COM(2009)567 final

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, *A Digital Agenda for Europe. Brussels: European Commission*, COM(2010)245 final/2

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, *Europe 2020 Flagship Initiative Innovation Union*, COM(2010)546 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI, *Un approccio globale alla protezione dei dati personali nell'Unione europea*, COM(2010) 609 def.

COMMUNICATION FROM THE COMMISSION, *Europe 2020: A strategy for smart, sustainable and inclusive growth*, COM(2010)2020 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI, *Dati aperti. Un motore per l'innovazione, la crescita e una governance trasparente*, COM(2011) 882 def.

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI, *Salvaguardare la privacy in un mondo interconnesso. Un quadro europeo della protezione dei dati per il XXI secolo*, COM(2012) 9 def.

COMMISSIONE EUROPEA, *Proposta di Direttiva del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati*, COM(2012) 10 def.

COMMISSIONE EUROPEA, *Proposta di Regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)*, COM(2012) 11 def.

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI, *Piano d'azione "Sanità elettronica" 2012-2020 – Una sanità innovativa per il 21esimo secolo*, COM(2012) 736 def.