Elsevier Editorial System(tm) for Journal of Biomedical Informatics

Manuscript Draft

Manuscript Number: JBI-18-875

Title: The European cross-border health data exchange roadmap: case study in the Italian setting

Article Type: SI: Personal Health Records

Keywords: Cross-border health data exchange, interoperability, ethics, regulatory issues, cybersecurity

Corresponding Author: Mrs. Giuliana Faiella,

Corresponding Author's Institution: Fondazione Santobono Pausilipon

First Author: Marco Nalin

Order of Authors: Marco Nalin; Ilaria Baroni; Giuliana Faiella; Maria Romano; Flavia Matrisciano; Erol Gelenbe; David M Martinez; Jos Dumortier; Pantelis Natsiavas; Kostas Votis; Vassilis Koutkias; Dimitrios Tzovaras; Fabrizio Clemente

Abstract: Health data exchange is a major challenge due to the sensitive information and the privacy issues entailed. Considering the European context, in which health data must be exchanged between different European Union (EU) Member States, each having a different national regulatory framework as well as different national healthcare system structures/organizations, the challenge is even greater. Europe has tried to address this challenge by launching in 2008, the epSOS ("Smart Open Services for European Patients") project, which was a European large-scale pilot on cross-border sharing of specific health data and services. The adoption of the framework for cross-border health data exchange proposed in epSOS is progressing, with most Member States planning the implementation of this framework by 2020. Yet, this framework is quite generic and leaves a wide space to each Member State regarding the definition of roles, processes, workflows and especially the specific integration with the National Infrastructure for eHealth. The aim of this paper is to present the current landscape of the evolving eHealth infrastructure for cross-border health data exchange in Europe as a result of past and ongoing initiatives, and illustrate challenges, open issues and limitations through a specific case study describing how Italy is approaching its adoption and accommodates the identified barriers. The paper discusses ethical, regulatory and organizational issues, while it focuses technical aspects such as interoperability and cybersecurity, as applicable in this context. Regarding cybersecurity aspects per se, we present the approach of the KONFIDO EU-funded project, which aims to reinforce trust and security in European cross-border health data exchange by leveraging novel approaches and cutting-edge technologies, such as homomorphic encryption, photonic Physical Unclonable Functions (p-PUF), a Security Information and Event Management (SIEM) system, and blockchain-based auditing. In particular, we explain how KONFIDO will test its outcomes through a dedicated pilot based on a realistic scenario, in which Italy is involved in health data exchange with other European countries.

Keywords: Cross-border health data exchange, interoperability, ethics, regulatory issues, cybersecurity.

Suggested Reviewers: Angelina Kouroubali
Foundation for Research and Technology - Hellas (FORTH)
kouroub@ics.forth.gr

Alexander Berler
IHE-EUROPE
a.berler@gnomon.com.gr

Pascal Coorevits
Ghent University
Pascal.Coorevits@UGent.be

Opposed Reviewers:

Research Data Related to this Submission

There are no linked research data sets for this submission. The following reason is given:
No data was used for the research described in the article

Cover Letter

Dear Guest Editors of the JBI Special Issue “The Vision of Personally Managed Health Data: Barriers, Approaches and Roadmap for the Future”,

The submitted manuscript entitled "*The European cross-border health data exchange framework: case study in the Italian setting*" constitutes a **Special Communication** authored by Marco Nalin, Ilaria Baroni, Giuliana Faiella, Maria Romano, Flavia Matrisciano, Erol Gelenbe, David Mari Martinez, Jos Dumortier, Pantelis Natsiavas, Kostas Votis, Vassilis Koutkias, Dimitrios Tzovaras and Fabrizio Clemente.

The manuscript refers to the current landscape of the evolving eHealth infrastructure for cross-border health data exchange in Europe and illustrates challenges, open issues and limitations through a specific case study describing how Italy is approaching the adoption and deployment of this infrastructure. While the major focus of the manuscript is given on technical aspects, such as interoperability and cybersecurity, we also discuss ethical, regulatory and organizational issues, which are applicable in this context. Focusing on cybersecurity aspects per se, the manuscript presents a novel approach elaborated in the scope of the KONFIDO EU-funded project, which aims to reinforce trust and security in European cross-border health data exchange by leveraging novel approaches and cutting-edge technologies through an integrated toolset.

We believe that the manuscript is relevant with the particular Special Issue and that it may constitute a useful contribution for the audience of JBI, as it presents through a timely viewpoint challenges as well as our experiences on health data exchange among European countries.

We would like to declare that the content of the paper is original and that it has not been published before.

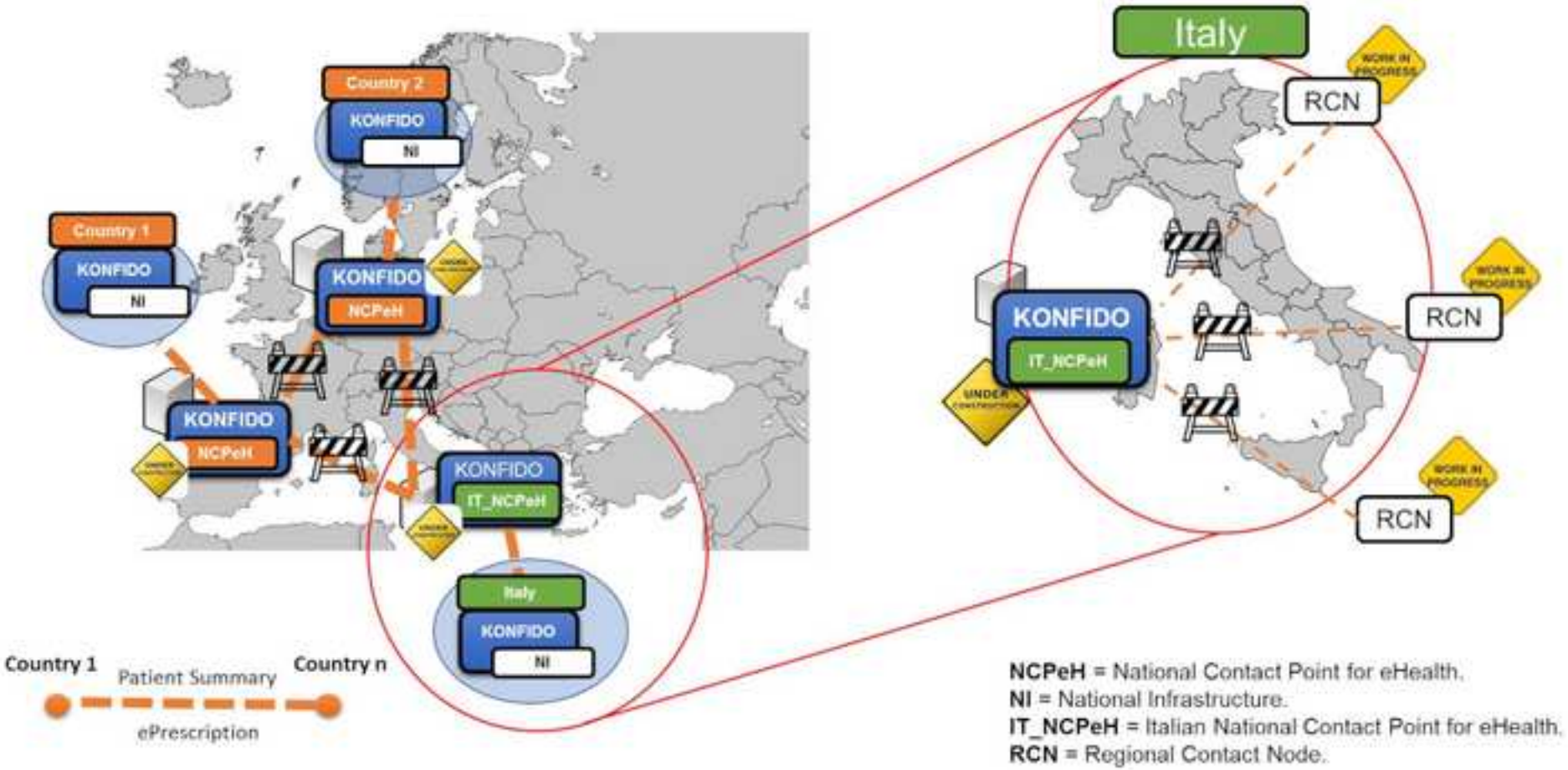
We are at your disposal for anything you may need concerning this submission and we look forward to receiving the peer-review comments.

Thank you very much for considering our work for potential publication in this Special Issue of the *Journal of Biomedical Informatics*.

Sincerely yours,

Giuliana Faiella
Fondazione Santobono Pausilipon
Email: giuliana.faiella@gmail.com

Graphical Abstract



Highlights

- Efficient cross-border health data among countries is a major priority in the European Union.

- Long lasting efforts have been devoted to establish a EU-wide, common infrastructure for cross-border health data exchange.

- Besides technical aspects, such as interoperability and cybersecurity, the deployment of such an infrastructure entails various challenges from the ethical, legal and organizational viewpoints.

- State-of-the-art technologies, such as homomorphic encryption, photonic Physical Unclonable Functions key generation, and blockchain-based auditing embodied in the evolving eHealth infrastructure may reinforce its security and user acceptance.

*Manuscript
Click here to view linked References

The European cross-border health data exchange roadmap: case study in the Italian setting

Marco Nalin[1], Ilaria Baroni[1], Giuliana Faiella[2], Maria Romano[1], Flavia Matrisciano[2], Erol Gelenbe[3], David Mari Martinez[4], Jos Dumortier[5], Pantelis Natsiavas[6], Kostas Votis[7], Vassilis Koutkias[6], Dimitrios Tzovaras[7], Fabrizio Clemente[8]

[1]Telbios S.r.l, Milan, Italy, [2] Fondazione Santobono Pausilipon, Naples, Italy, [3]Department of Electrical and Electronic Engineering, Imperial College of Science, Technology and Medicine, London, UK, [4]Eurecat - Centro Tecnológico de Catalunya, Barcelona, Spain, [5]Time.lex, Brussels, Belgium,[6]Institute of Applied Biosciences, Centre for Research & Technology Hellas, Thermi, Thessaloniki, Greece, [7]Information Technologies Institute, Centre for Research & Technology Hellas, Thermi, Thessaloniki, Greece, [2-8]Insitute of Cristallography - CNR, Rome, Italy

Corresponding: Giuliana Faiella

Present address: giuliana.faiella@gmail.com

Abstract:

Health data exchange is a major challenge due to the sensitive information and the privacy issues entailed. Considering the European context, in which health data must be exchanged between different European Union (EU) Member States, each having a different national regulatory framework as well as different national healthcare system structures/organizations, the challenge is even greater. Europe has tried to address this challenge by launching in 2008, the epSOS ("Smart Open Services for European Patients") project, which was a European large-scale pilot on cross-border sharing of specific health data and services. The adoption of the framework for cross-border health data exchange proposed in epSOS is progressing, with most Member States planning the implementation of this framework by 2020. Yet, this framework is quite generic and leaves a wide space to each Member State regarding the definition of roles, processes, workflows and especially the specific integration with the National Infrastructure for eHealth. The aim of this paper is to present the current landscape of the evolving eHealth infrastructure for cross-border health data exchange in Europe as a result of past and ongoing initiatives, and illustrate challenges, open issues and limitations through a specific case study describing how Italy is approaching its adoption and accommodates the identified barriers. The paper discusses ethical, regulatory and organizational issues, while it focuses technical aspects such as interoperability and cybersecurity, as applicable in this context. Regarding cybersecurity aspects per se, we present the approach of the KONFIDO EU-funded project, which aims to reinforce trust and security in European cross-border health data exchange by leveraging novel approaches and cutting-edge technologies, such as homomorphic encryption, photonic Physical Unclonable Functions (p-PUF), a

Security Information and Event Management (SIEM) system, and blockchain-based auditing. In particular, we explain how KONFIDO will test its outcomes through a dedicated pilot based on a realistic scenario, in which Italy is involved in health data exchange with other European countries.

Keywords: Cross-border health data exchange, interoperability, ethics, regulatory issues, cybersecurity**.**

1. INTRODUCTION

Patient data exchange among healthcare organizations is a significant challenge due to the sensitive information and the privacy issues involved. In Europe, the right of a patient for cross-border healthcare is defined in Directive 2011/24/EU [1] of the European Parliament and of the Council of 9 March 2011. However, in practical terms cross-border healthcare is quite complicated, since each European country has its own national regulatory framework as well as its National Healthcare System structures/organizations/roles, etc., hampering efficient health data exchange.

Thus, this paper outlines the current landscape regarding the establishment and deployment of an interoperable and secure cross-border health data exchange framework in Europe. First, it outlines the strategy that the Europe Union (EU) has undertaken since 2008 to build a framework for interoperable exchange of eHealth information within EU Member States (starting from a Patient Summary and the ePrescription services) through the epSOS (European Patients – Smart Open Services) initiative [2]. Despite establishing a basic, common framework for EU Member States, its adoption by the different Member States requires time and effort and therefore several key barriers are identified. Furthermore, the paper presents the adoption of epSOS in Italy, which is particularly interesting because of its federated healthcare system, where "regions" are the actual actors involved in the management of patients' data. Besides technical aspects, the paper discusses important challenges concerning, legal, organizational and ethical issues, which are also applicable in this context. As more actors are involved in the exchange of personal health data, important cybersecurity threats may arise also related with societal and ethical implications. To this end, the paper introduces the approach followed by the KONFIDO ("Secure and Trusted Paradigm for Interoperable eHealth Services") EU-funded project [3]-[4], which develops tools and procedures to reinforce the security of cross-border health data exchange across EU Member States. In particular, KONFIDO leverages novel approaches and cutting-edge technologies, such as homomorphic encryption, photonic Physical Unclonable Functions (p-PUF), a Security Information and Event Management (SIEM) system, and blockchain-based auditing. By analysing the security threats that may affect this common infrastructure [5], KONFIDO plans a pilot against Italian National infrastructure to validate its innovative toolset, taking into account the major regulatory, ethical and technical barriers identified.

2. BACKGROUND

In 2008 the epSOS initiative was launched in Europe, involving initially a few stakeholders, but gradually expanded to a large-scale pilot encompassing 25 countries and 50 beneficiaries. The initiative was partially founded by the ICT Policy Support Programme (ICT PSP), as part of the Competitiveness and Framework Programme by the European Commission, and it was completed in 2014. The main goal of epSOS was to develop a practical eHealth framework and an Information & Communication Technology (ICT) infrastructure for enabling interoperable access to patient health information, with respect to basic Patient Summaries (PS) and ePrescriptions (eP) between different EU healthcare systems. In particular:

- The **PS** is a standardized set of patient data including:
    - General information about the patient (name, birth date, gender, etc.);
    - A medical summary consisting of the most important patient data (e.g., allergies, current medical problems, etc.);
    - A list of current medication including all prescribed medication that the patient is currently taking;
    - Information about the PS itself (e.g., when and by whom was the PS generated or updated).
- **The eP** includes two main processes:
    - the electronic prescription of drugs, transmitting the information to the pharmacy where it is being retrieved;
    - eDispensing (eD), i.e. the retrieval of an eP, and dispensing of the drug to the patient, and the submission of a report for the medicine dispensed.

With a special focus on interoperability, a major challenge was to map all the selected coding systems used in PS and eP into a common coding. If a country used a different coding system, a specific component needs to be deployed to convert the national coding system to the epSOS coding system.
In the vision proposed by epSOS, each country must deploy a National Contact Point (NCP) for eHealth (NCPeH), which is an organization delegated to act as a bidirectional interface between the existing national functions provided by the national IT infrastructures and those provided by the common European infrastructure. Besides the already mentioned semantic interpretation and translation, the NCP also acts as a kind of mediator as far as the legal and regulatory aspects are concerned, as explained in the following paragraph.

3. LEGAL, ORGANIZATIONAL AND ETHICAL IMPLICATIONS FOR CROSS-BORDER IN EUROPE

3.1 Legal and organizational aspects

From a legal point of view, providers of cross-border eHealth must comply with Directive 2011/24/EU on patients' rights in cross-border [6]. The Directive specifies the rights (i.e., the right to access data, the right to erase and correct data and the right to know who accessed data) and the rules for accessing healthcare in another EU country and one of its tasks is, precisely, to make sure that the European eHealth systems attains "a high level of trust and security". A key provision of the Directive is the creation of NCPs that must have facilities to provide the information and practical assistance to patients needed to make an informed decision.

Patients should look at the NCP of their own country, as well as the one of that country where they are thinking of going to access healthcare services to check the credentials of the health professional they are thinking of using. Moreover, patients who have received treatment in another Member State are entitled to a copy of the medical record (Article 4(2)(f)). It is a responsibility of the Member States to ensure that there are complaints procedures and mechanisms in place for patients to seek remedies, if they suffer harm arising from the healthcare they receive. Remedies are in accordance with the legislation of the Member State of treatment.

The NCPs must also provide patients with information on the list of information that should appear in cross-border prescriptions. Specifically, the information on the prescriptions should make it easier for patients to understand the prescription and instructions for use. A non-exhaustive list of information that should be included in a cross-border prescription is contained in the annex of the implementing Directive [7].

Cross-border exchange of health data is regulated by European and national legal rules regarding the protection of personal data. Currently, this domain is governed by the General Data Protection Regulation (2016/679/EC) [8].

Cross-border exchange of electronic health records (EHRs) is not possible without a secure identification of patients and healthcare providers. The main legal instrument at the EU level in the area of cross-border electronic identification is Regulation (EU) 2014/910 (the "eIDAS Regulation"). The first part of this Regulation introduces a mechanism of mutual recognition of notified electronic identification schemes between Member States.

The international or cross-border transfer of information raises interesting issues regarding the need for a harmonization of rules, processes and safeguards both in Europe and globally. In this sense, the EU is promoting activities in the field of eHealth interoperability and standardization. Specifically, the eHealth Network (eHN) has been created by the Directive 2011/24/EU to achieve coordination, coherence and consistency. It is co-chaired by the European Commission and Austria. It draws up

guidelines on how to apply patients' rights in cross-border healthcare. In general, the network aims to enhance interoperability between electronic health systems and continuity of care with guidelines on a minimum/non-exhaustive PS dataset for electronic exchange in accordance with the cross-border directive 2011/24/EU [9]. The new guidelines specify how patients, upon explicit request, can have a summary of their EHR available when visiting another country in the EU. Similar guidelines have been adopted by the eHN in 2014 for the eP minimal dataset [10].

To stimulate the development of generic cross-border eHealth services, 16 Member States received financial support under the Connecting Europe Facility (CEF). CEF is a key EU funding instrument [11] of the Innovation and Networks Executive Agency (INEA), aiming to promote growth, jobs and competitiveness through targeted infrastructure investment at European level, supporting interconnected trans-European networks in the fields of transport, energy and digital services. CEF is the financial framework under which the eHealth Digital Service Infrastructure (eHDSI) initiative is carried out, and the eHN guidelines are the reference for the electronic exchange of health data adopted by eHDSI. The eHealth Digital Service Infrastructure (eHDSI or eHealth DSI) is the initial deployment and operation of services for cross-border health data exchange [12], meant as a move from the epSOS conceptual framework to its deployment phase. Whenever real patient data are exchanged, the NCPeH must be in conformity with the agreed principles as adopted by the eHN.

In 2015, a "Joint Action to Support the eHealth Network" (JASeHN) was launched to support eHN. In JASeHN public health authorities and other stakeholders of all Member States are currently collaborating and developing recommendations for the eHN. An important document produced by JASeHN and adopted by eHN in 2017 is the "Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth on the Criteria required for the participation in Cross-Border eHealth Information Service" [13]. According to this agreement, cross-border exchange of health data can only happen when the Member States involved enter into an agreement for this specific purpose. The agreement will have its legal basis in the national law of the respective Member State. In particular, the agreement determines the following important points:

- The mechanisms of identification of patients, health professionals and healthcare providers have to follow the eIDAS Regulation.
- Country B shall ensure that only health professionals authorized according to its national law may have access to patients' data concerning health.
- Each Contracting Party shall designate one NCPeH to act as a single communication gateway with the NCPeH designated by other Contracting Parties.
- Each Country is responsible for the accuracy and integrity of semantic processing.
- Each Contracting Party shall ensure the compliance of its NCPeH with the principles of data protection by design and by default, the requirements for confidentiality, integrity, authenticity,

availability, non-repudiation, encryption, logs, audit trails, and other means of data security and control measures in compliance with Regulation 2014/910/EU and Regulation 2016/679/EU.

In the following, the Table 1 summarizes the main legal and organizational requirements previously described and the barriers to their applications.

Table 1 - Legal and Organizational Requirements and Barriers

3.2 Ethical aspects

In order to understand what ethical principles have already been identified and discussed in the context of eHealth and cross-border health data exchange, a comprehensive analysis of recent literature and European Regulations has been conducted [14]. In [Figure 1, the main findings are aggregated for similarity of concepts and goals identifying a minimum dataset of ethical principles for cross-border applications. [Table 1 translates the ethical principles into pragmatic actions to explain how the abstract ethical principles may be included and implemented into cross-border solutions designed according to the "ethics-by-design" principle [14].

[Figure 1: Aggregation of literature findings about ethical principles related to eHealth and cross-border health data exchange (updated from [14])]

[Table 1 - Ethical principles and suggested actions]

In the following, the Table 3 summarizes the main ethical requirements previously described and the barriers to their applications.

[Table 2 - Ethical requirements and barriers]

4. THE EUROPEAN INFRASTRUCTURE FOR CROSS-BORDER HEALTH DATA EXCHANGE

The eHN released the "Guideline on an Organisational Framework for eHealth National Contact Point" [15]. The main architectural element of this framework is the NCPeH, which constitutes the country's communication gateway that assures the interface (not only technical) between the National Infrastructure (NI) and the EU network of other Member States' NCPeH, as well as with the central EU services. The NCPeH must be then recognizable both in the EU domain (with the NCPeH of other countries) and in the national domain, acting as the main interface between the two.

Every NCPeH can work in two different scenarios, when a patient is travelling abroad for any reason (holiday, study, work relocation, etc.):

- Country-A: It is the Country of Affiliation, i.e., the country which holds information about a patient, where the patient can be univocally identified and where his/her data may be accessed;
- Country-B: It is the Country of Treatment, i.e., the country where cross-border healthcare is provided, when the patient is seeking care abroad.

Different EU Member States will deploy their NCPeH in different moments, based on the eHDSI NCPeH service deployment plan [16].

In Italy, the implementation of this infrastructure was carried out through a project of the Italian Ministry of Health, the Digital Agency (AgID – Agenzia per l'Italia Digitale) and three pilot regions (Lombardy, Veneto and Emilia-Romagna). The project, funded by CEF, is called "Deployment of Generic Cross Border eHealth Services in Italy" (call: eHealth 2015 CEF-TC 2015-2) [17] and started on January the 1st 2017, ending in 2020. It includes the following activities:

- Governance and Management
- NCPeH architectural design
- NCPeH development and deployment
- Communication and training strategy

In the cases in which Italy acts as the Country of Affiliation (Country-A) of a patient abroad, the NCPeH should retrieve the PS or the eP, first with a verification of the patient's consent in the EHR (infrastructure at the national level, and then the relevant documents in the Regional Systems [18].

On the other hand, when Italy is acting as the Country of Treatment (Country-B) for a foreign patient that needs to provide the PS or eP, the NCPeH will provide a dedicated portal which will forward the request to the NCPeH of the respective Country of Affiliation (Country A), receive the documents, translate them in Italian and provide the tools to the healthcare professional or pharmacist.

The NCPeH itself currently will remain in pre-production phase until a proper audit and test from the eHN can occur: after these steps, the NCPeH will enter the production phase and will be fully activated.

A project which is relevant in the creation of the Italian National Infrastructure and is influencing the deployment of the NCPeH is the IPSE [19] ("European and National Interoperability solutions for the Electronic Healthcare Record: Patient Summary and ePrescription components" / Interoperabilità europea e nazionale delle soluzioni di fascicolo sanitario elettronico: componenti Patient Summary e ePrescription). IPSE was carried out by the Italian Ministry of Health and 10 Italian Regions between

2010 and 2012, and it started the definition of a National Interoperability infrastructure based on the epSOS concepts. In particular, together with the NCPeH node, IPSE defined an Interregional Contact Node (ICN), coordinating a set of Regional Contact Nodes (RCN) to be implemented by each Region, with a similar federated model with respect to the one defined by the eHN between EU Member States. [Figure 2 illustrates the IPSE infrastructure.

[Figure 2: The IPSE infrastructure based on epSOS (new nodes were defined, in particular the Interregional Contact Node (ICN) and Regional Contact Nodes (RCN)) (Adapted from [19])]

Moreover, IPSE defined reusable epSOS building blocks [20], in particular:

- The legal framework.
- End-2-end security, in particular:
    - VPN based on SHA-2 certificates.
    - Encrypted and signed messages.
    - No data storage at NCP level.
    - Audit trail for every transaction.
- Adoption of IHE (Integrating the Healthcare Enterprise) profiles.
- Semantic Interoperability.

5. THE ITALIAN eHEALTH DATA INFRASTRUCTURE

The Italian healthcare system is based on a national framework called National Healthcare Information System (Nuovo Sistema Informativo Sanitario - NSIS), where regulations and a unified EHR are defined at the national level. However, as the Italian healthcare system is organized as a federation of Regions, all the implementations, deployment plans, data collection and management are developed at the regional level.

The Agency in charge of Italy's Digitalization (AgID), in cooperation with the Ministry of Health and the Ministry of Economy and Finance designed the National Interoperability Infrastructure (*Infrastruttura Nazionale per l'Interoperabilità - INI*) to exchange information among the different Regions and speed-up the deployment of EHR for Regions. The national EHR in Italy is called Fascicolo Sanitario Elettronico (FSE), and it will be implemented by each Region, following national rules within the technological framework of the Healthcare Insurance card - *Tessera Sanitaria (TS System)*. Currently, the FSE is not activated and implemented in all Italian regions [21]. The National regulation on FSE [22] defines the content of the specific implementations: all healthcare data about the patient, laboratory records, therapies, medical history (documents that are part of the FSE), provisions for the protection of the privacy of the patients, the governance system, data collection process, the data encoding systems. Furthermore, it contains an essential version of the FSE which is called Profilo

Sanitario Sintetico or Patient Summary (PS), which includes the same information of the Patient Summary defined in epSOS and by the eHDSI. The PS is managed by the GP (general practitioner or paediatrician for children), which has the responsibility to update it with administrative and medical information.

For citizens, the FSE is activated with the signature of the informed consent to allow the processing of personal data and the consultations by authorized operators of the healthcare system. This step enables the citizen to consult his/her healthcare records with his/her entire clinical history, and to share this information with healthcare professionals. Two activation paths are implemented from the Regions: from the GP's office, or through a dedicated online portal with proper authentications (with the Public System for Digital Identity – SPID). In both cases, the citizen will sign the informed consent, which explains what the FSE, what its activation means, its purposes, who has permission to consult it and who will update it. Access to FSE is enabled by means of personal credentials and access procedures, established by national law and applied autonomously by the Regions. In particular, the FSE Minimum Dataset and the relevant documents included are listed in Table 4.

[Table 3: FSE documents according to dPCM n. 178/2015, differentiating the minimum data set and the extended data set [22]]

The complete picture for the Italian Health National Infrastructure, including all the components needed for cross-border health data exchange (e.g., NCPeH) is presented in Figure 3.

[Figure 3: Italian eHealth data Infrastructure]

In [Figure 3, we can differentiate four levels:

1) **At the European level**: the NCPeH will be instantiated within 2020, allowing Italy to act both as Country-A and Country-B in the data exchange defined in epSOS. This node will follow the standards defined by eHDSI and it will become operational after appropriate testing and auditing processes (NCPeH).

2) **At the National level**: the NCPeH node will contact the National Interoperability Infrastructure (INI) to route the requests in the relevant Region. INI will orchestrate the data exchange with all the Regions. In the second quarter of 2018, 17 Regions are declared active in trying to implement their own FSE system, while 11 of them are already connected with the INI network [21].

3) **At the Regional level**: the specific Regional FSE system. There are two different models for the Regional level. In the first model, the documents index and the documents themselves are in the same (Regional) system (saved in structured or unstructured format: HL7 CDA v2 or PDF). In the second

model, the Regional system is composed only by the clinical documents' index (including metadata), while all the documents are shared in the different Document Repositories in the territory (Hospitals, GPs, etc.).

4) **At the Local level**: we can find all the end-users of the system, being both Italian citizens accessing eHealth services or Healthcare Professionals dealing with patients.

The INI node, which is in charge for the exchange of any clinical document between Regions, has a defined set of processes to be managed: patient identification, consent management, document search, document retrieval, meta-data management (creation, update, deletion), documents' reference retrieval, index transfer (to another Region). This node relies on the National Health Card System (Tessera Sanitaria – TS System) for the identity information of the patient.

In Italy, the PS is a subset of information of the FSE, and it is an actual clinical document exchanged like all the other clinical documents in Italy. It must be prepared by the treating GP of the patient and it must include: patient and GP IDs, list of diseases, diagnosis, allergies, pharmacological therapies, chronic conditions and all the information needed to guarantee the patient care. In case of GP's change, the new GP will have the responsibility to update the PS, with his ID and updated information about the patient.

ePrescription ([Figure 3) follows two separate flows (regulated by the Ministry Decree of the 2nd November 2011), which is in line with the European system:

- The eP of a drug consists in the release of a unique number (Numero di Ricetta Elettronica – NRE), issued by the SAC (Sistema di Accoglienza Centrale – a subsystem of the TS System), which allows doctors, pharmacies, and public or private structure to exchange information on the prescription in real time. GPs have the possibility to issue a paper version of the prescription in case of system malfunctions. In some cases, there is a Regional node releasing the NRE (called SAR), which interacts with the SAC to make sure that there is alignment between the two systems.
- The eD, where the drug is released, and the information is forwarded to the National Health Smart Card System, again by the NRE. Using the NRE and the fiscal code, the dispenser forwards the communication to the SAC/SAR to recover the treatment or the drug that the patient needs, and when the eD is closed, he/she sends the economical information back to the SAC/SAR with the eventual costs paid by the patient.

Table 5 recalls the legal, organizational and ethical requirements identified in Table 1 and Table 2. For each of them describes the solutions applied in the Italian context at each level of Figure 3.

[Table 4 – Legal, Organizational and Ethical Requirements and solutions that will be implemented in Italy at European and National/Regional Level]

6. REINFORCING SECURITY OF THE EU eHEALTH DATA INFRASTRUCTURE THROUGH THE KONFIDO TOOLSET

KONFIDO is an EU-funded research project aiming to develop a holistic paradigm for secure cross-border health data exchange. It builds its solution upon existing/evolving European frameworks, such as OpenNCP (Open-source and reference version of the NCP software) [23]-[24]-[25], which is the open-source National Contact Point (NCP) software implementation of its predecessor project epSOS, and eIDAS (electronic IDentification, Authentication and trust Services) [22], which stands for the EU regulation on electronic identification and trust services for electronic transactions in the internal market. In epSOS, the security of communications is ensured by employing cryptography and appropriate protocols. However, the security of communicating parties is not enforced by technical means; it is instead pretended by legally binding agreement. Furthermore, epSOS does not offer any protection against the propagation of cyber-attacks. Therefore, attacks which succeed in compromising a National Infrastructure (NI) can exploit the NCP to propagate to other countries. This means that, due to this chain of trust between the NCPs, if one NCP states that someone is authenticated, this will be accepted by the NCPs of other countries. In particular, the PS is retrieved in plain text. This means that a vulnerability of NCP can generate a data breach on the OpenNCP processes.

KONFIDO developed a toolset which can be used to overcome the identified vulnerabilities by deploying a set of functionalities to guarantee, for example, that the medical data will be never exposed as plain-text in a non-secure area. KONFIDO improves OpenNCP security with a set of security tools organized in an easily pluggable architecture [25]. Specifically, the toolset offered by KONFIDO includes the following tools/services:

- *Trusted Execution Environment* (TEE): the new security extensions provided by some of the main CPU vendors; focuses on the enhancement of the NCP Connector, the component that translates the PS. During the PS translation, the healthcare data may be exposed to attacks (for example, dumping the memory of the OpenNCP process in charge of document transformation processing). KONFIDO aims to protect the sensitive information with a manipulation of the PS inside the TEE [26].
- *Physical Unclonable Function* (PUF)-based security solutions that rely on photonic technologies to generate strong keys [27]-[28]; PUF keys are used to establish secure communication links between NCP nodes and/or other KONFIDO modules.
- *Homomorphic Encryption* (HE) mechanisms; The HE component is used to protect the exchange and the processing of patient data at NI level and in the context of NCP [29].

- Customized extensions of *Security Information and Event Management* (SIEM) solutions [30]; will be able to analyze information and events collected using a holistic approach at the different levels of the monitored system to discover possible ongoing attacks, or anomalous situations.
- *Blockchain-based auditing*: a set of disruptive logging and auditing mechanisms developed in other technology sectors and transferred to the healthcare domain [31]; enables to prove that healthcare data have been requested by a legitimate entity and whether they have been provided or not. The events stored are referred to National Infrastructure to retrieve patient data from the national healthcare system and NCP to exchange and visualize the PS.
- A customized *eIDAS implementation*; eIDAS-compliant authentication will target patients, that could access the system using an eIDAS cross-border authentication to provide consent in a not repudiable manner [32]-[33].

The EU's recommendations for the last few years [8] have tended to stress the protection of privacy and security of individuals and organizations in the domain of cyberspace. Healthcare is obviously a critical area, because it also deals with individuals and organizations that are more vulnerable than the general public. As a cybersecurity project that targets the security of the field of transnational, European healthcare support systems, KONFIDO aims to reinforce the security measure of OpenNCP [34], also by detecting and mitigating its potential misuse, e.g. malicious attacks [35]-[36]-[37]. To first detect and then counter a misuse, monitoring and control actions can be taken within the system, both at the node that makes the request (A), and at the receiver node (B). For each attempted use of the system we propose that such controls be carried out by both A and B [35]. Further controls can also be carried out at the overall system level, where data from the lower levels can be integrated. Also, attempts at misuse, when detected and rejected, may come back, as similar attacks or in some form of disguise. Thus, detections and rejections will be utilised again for similar behaviours, leading to the potential of applying machine learning techniques to enhance the results. However, this comes at a cost with added load and congestion on the detection and mitigation system, since repeated attack attempts under different guises will create overload in different system components. Even with perfect detection and rejection systems, detection and cybersecurity control schemes themselves will create additional workload and possible congestion, which will need to be evaluated, quantified, and for which resources have to be provisioned during normal system operations [35].

Detection schemes are obviously imperfect and will result in some false alarms. Thus, their evaluation should include the costs of these false alarms, including the additional delays, and possible user dissatisfaction and frustration caused by false alarms. Therefore, an overall cost/benefit evaluation of misuse and attack detection schemes is a useful direction of further research.

6.1 KONFIDO deployment in italy

In order to demonstrate the KONFIDO functionalities in the Italian context, a user scenario and a pilot study have been defined, in which Italy acts as the Affiliated Country. Besides the above, this section refers to the foundations of the respective validation framework.

6.2 The Italian Scenario: An example

Anna is from Italy, Lombardy region, and she is in vacation in Spain. Thanks to KONFIDO, Anna knows that in case of problems, any certified healthcare professionals in Barcelona will have access to her PS in a secure way. During the journey, Anna faints and decides to go to the nearest hospital in Barcelona to check her health conditions. The healthcare professional of the hospital (Local Point of care) connects to the Spanish NCPeH and identifies and authenticates Anna and his/herself using eIDAS. The action of authentication, request the retrieval of Anna's PS are all enhanced by KONFIDO. The retrieval request is sent to the Italian NCPeH that, using the National Interoperability Infrastructure (INI) node of the national architecture of the FSE, performs the following actions:

- Verifies Anna's personal data and the validity of consent to send clinical data abroad.
- Interconnects to the Lombardy regional systems.
- After the verification of consent, the FSE regional system retrieves the required clinical documents from a document repository.
- Then, a specific component of the NCPeH, called National Connector transforms in a Trusted Execution Environment the Italian Synthetic Health Profile into a PS syntactically compatible with European specifications.
- Finally, a dedicated portal enables the health professional to visualize the document.

6.3 The Italian Pilot: Scenario implementation

As the actual Italian National Infrastructure is not available to a research project such as KONFIDO as a test-bed for malicious misuses of the system, unintentional misuses of the system and actual system attacks, the project will realize a testbed which will support the piloting activities of the developed technologies. This testbed will be composed by a mix of KONFIDO security components and software stubs, i.e. prototype software artifacts implementing the same interfaces of the existing components (or those currently under development/test by the Italian Ministry of Health).

The Italian testbed architecture is illustrated in [Figure 4, and it is composed of:

- A KONFIDO-enhanced OpenNCP deployment, simulating the Italian NCPeH. This node will be responsible for the exchange of the information between the other KONFIDO testbeds (which will be deployed in Spain and Denmark) and the Italian National Infrastructure.

- A prototype Web portal of OpenNCP for Italian clinicians who may wish to retrieve a foreign patient's PS and eP.;
- A stub component which acts as the INI, replicating its processes for the interregional communications and exchange of medical information.
- Two Regional stub components, which KONFIDO enhances, simulating Regional FSE (containing the Patient Summaries and ePrescription).

[Figure 4: Italian Test-bed for the KONFIDO Pilot]

Table 6 recalls the legal, organizational and ethical requirements identified in Table 1 and Table 2. For each of them describes the solutions applied in the Italian pilot of Figure 4.

[Table 5 - – Legal, Organizational and Ethical Requirements and solutions that will be implemented in the Italian Pilot]

While the main goal of KONFIDO is to secure the OpenNCP nodes of Member States, the secondary goal of testing some of the security enhancements also at Regional level can be pursued in parallel, and the rationale for this is provided by the IPSE project, the aim of which is to reuse epSOS building blocks also within the INI.
This testbed will be used for the definition of test use cases and misuse cases, both from external attackers and malicious insiders in the involved systems.

6.4 Pilot validation

Pilot validation aims to verify that the KONFIDO solution meets the project objectives, based on data gathered during the pilot phase. The main goal is to prove the following three objectives:

1. The KONFIDO solution actually works.
2. KONFIDO can be integrated with pilot countries' national infrastructure (i.e. EHR systems etc.).
3. The KONFIDO solution improves the security of exchanging information through OpenNCP.

As part of the validation phase, the activities conducted in the KONFIDO pilots will be reported in detail and the gathered data will also be presented. In order to provide tangible evidence of achieving the three validation objectives, a set of measurable criteria are going to be defined based on the data collected from pilots, as explained in [Table 6. The pilot validation criteria will be based on the following axes:

- User goals as the main result of the KONFIDO user requirements phase [36].
- Misuse cases identified as main threat scenarios.
- Standards and widely accepted best practices.
- The exact validation criteria will be iteratively elaborated during the pilots' phase as they heavily depend on the data collected. However, the following Table 7 depicts some indicative criteria defined as part of the pilot validation planning process.

[Table 6: Preliminary criteria for pilot validation]

The ultimate goal of the validation phase is to confirm that the KONFIDO objectives were successfully met. Lessons learned and challenges will also be elaborated to produce the final validation conclusions and identify opportunities for future work as well as a strategy for the transferability of the KONFIDO outcomes to other EU Member States.

7. DISCUSSION AND CONCLUSION

The development of a unified European framework for the exchange of health-related data is a critical problem that needs to be solved, in order to match the regulatory frameworks at the European level and within the Member States and because of the sensitive information that is exchanged. Thus, a "privacy by design" approach must also be undertaken to generate trust in the potential end-users and unlock eHealth potential and facilitate the framework's adoption across Europe.

The European Commission has tried to address the issue of cross-border exchange of health data with the epSOS project, and with several other initiatives following its proposed model. However, the actual adoption and implementation of this model requires time and effort to be given by EU Member States, in order to define appropriate processes, regulations and technological infrastructures. In this context, the major barriers identified can be summarized as follows [39]:

- The Member States are not all aligned with JASeHN agreement.
- Different consent mechanisms among Member States.
- Lack of standard electronic health record-system among Member States.
- Different implementation of EU regulations among Member States.
- Different information workflows among National Infrastructure and healthcare organizations.
- Lack of harmonization of rules, processes and safeguards.
- NCPeH are still in early stages.
- Lack of the budget to address security aspects by healthcare organizations.

In this paper, we have described the process that Italy followed for the development of the epSOS model, implementing its own NCPeH in parallel with the development of the National EHR (called FSE). Since the Italian Healthcare System is federated and administered regionally, the implementation of the FSE is itself federated and each Region can deploy its own version [38]. This deployment is an ongoing process, which has a different level of maturity levels across Regions.

In this scenario of federations of different actors, both at Regional, National and European level, several threats to security and integrity of personal health data might arise. Thus, the KONFIDO project aspires to demonstrate how innovative technologies may be deployed in realistic scenarios that are compliant with legal and ethical principles [14]. To this end, KONFIDO project elaborated on a user requirements engineering phase in which key barriers and facilitators have been identified [36] and elaborated providing end-user goals and identify possible threats [35]. KONFIDO solution will be validated via pilots implemented in Italy, Denmark and Spain. The Italian pilot will implement a test-bed to validate the KONFIDO solution against near real-world conditions and also elaborate on methods to overcome the identified key barriers with customized eIDAS system and an enhancement the functionalities of OpenNCP in terms of consent management and security features, as described in details in Table 6.

FUNDING

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 727528 (KONFIDO - Secure and Trusted Paradigm for Interoperable eHealth Services).
This paper reflects only the authors' views and the Commission is not liable for any use that may be made of the information contained therein.

REFERENCES

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0024&from=EN. Accessed on 2 November 2018.

[2] epSOS project website. https://ec.europa.eu/digital-single-market/en/news/ cross-border-healthproject-epsos-what-has-it-achieved. Accessed on 2 November 2018.

[3] http://www.KONFIDO-project.eu/. Accessed on 2 November 2018.

[4] R. Martino, S. D'Antonio, L. Coppolino and L. Romano (2017). Security in Cross - Border Medical Data Interchange: A Technical Analysis and a Discussion of Possible Improvements. In:

Proceedings of the 41st IEEE Annual Computer Software and Applications Conference COMPSAC 2017.

[5] L. Coppolino, S. D'Antonio, L. Romano, M. Staffa. KONFIDO project: a secure infrastructure increasing interoperability on a systemic level among eHealth services across Europe. (2017). Proc. IEEE Int Conf Internet of Things (iThings) and Green Computing and Communications (GreenCom) and Cyber, Physical and Social Computing (CPSCom) and Smart Data (SmartData).;342–7. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.57.

[6] 2011/24/EU Directive on the application of patients' rights in cross - border healthcare (Cross - Border Directive).

[7] https://ec.europa.eu/health//sites/health/files/cross_border_care/docs/impl_directive_prescriptions_2012_en.pdf. Accessed on 2 November 2018.

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) ELI: http://data.europa.eu/eli/reg/2016/679/2016-05-04.

[9] https://ec.europa.eu/health/sites/health/files/ehealth/docs/guidelines_patient_summary_en.pdf. Accessed on 2 November 2018.

[10] https://ec.europa.eu/health/sites/health/files/ehealth/docs/eprescription_guidelines_en.pdf. Accessed on 2 November 2018.

[11] https://ec.europa.eu/inea/en/connecting-europe-facility. Accessed on 2 November 2018.

[12] https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/eHDSI+Mission. Accessed on 2 November 2018.

[13] https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20170509_co06_en.pdf. Accessed on 2 November 2018.

[14] G. Faiella G. et al. (2018) Building an Ethical Framework for Cross-Border Applications: The KONFIDO Project. In: Gelenbe E. et al. (eds) Security in Computer and Information Sciences. Euro-CYBERSEC 2018. Communications in Computer and Information Science, vol 821. Springer, Cham.

[15] https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20151123_co01_en.pdf. Accessed on 2 November 2018.

[16] https://ec.europa.eu/cefdigital/wiki/download/attachments/35210488/eHDSI_ServiceCatalogue-ServiceDelivery-OveralDeployment-Plan_V2.8_20180621.pdf?version=1&modificationDate=1530600169719&api=v2. Accessed on 2 November 2018.

[17] https://ec.europa.eu/inea/sites/inea/files/cef-tc-2015-2.pdf. Accessed on 2 November 2018.

[18]https://www.fascicolosanitario.gov.it/progettazione-realizzazione-e-collaudo-del-NCPeH-e-dei-servizi-transfrontalieri.

[19]http://www.arit.it/aree-tematiche/sanita-elettronica/86-il-progetto-ipse.html. Accessed on 2 November 2018

[20]http://www.promisalute.it/upload/mattone/documentiallegati/epSOS_13660_629.pdf. Accessed on 2 November 2018.

[21] https://www.fascicolosanitario.gov.it

[22] Decree of the President of the Council of Ministers - dPCM n. 178/2015

[23] M. Fonseca, K. Karkaletsis, I. Cruz, A. Berler, I. Oliveira. OpenNCP: a novel framework to foster cross-border e-health services. (2015). Stud Health Technol Inform.; 210:617–21. https://doi.org/10.3233/978-1-61499-512-8-617.

[24]M. Staffa, L. Coppolino, L. Sgaglione, E. Gelenbe, I. Komnios, E. Grivas, O.S.L. Castaldo: KONFIDO: An OpenNCP-based secure E health data exchange system. In: E. Gelenbe, P. Campegiani, T. Czachorski, S. Katsikas, I. Komnios, L. Romano, D. Tzovaras (eds.) (2018). Recent Cybersecurity Research in Europe: Proceedings of the 2018 ISCIS Security Workshop, Imperial College London. Lecture Notes CCIS No. 821, Springer Verlag

[25] M. Staffa, S. Sgaglione, G. Mazzeo, L. Coppolino, S. D'Antonio, L. Romano, E. Gelenbe, O. Stan, S. Carpov, E. Grivas, P. Campegiani, L. Castaldo, K. Votis, V. Koutkias, I. Komnios. An OpenNCP-based solution for secure eHealth data exchange. (2018). J Netw Comput Appl.;116(15):65–85. https://doi.org/10.1016/j.jnca.2018.05.012.

[26] L. Coppolino, S. D'Antonio, G. Mazzeo, L. Romano, L. Sgaglione. (2018). Exploiting New CPU Extensions for Secure Exchange of eHealth Data at the EU Level. 14th European Dependable Computing Conference (EDCC2018). DOI 10.1109/EDCC.2018.00015

[27] M. Akriotou, C. Mesaritakis, E. Grivas, C. Chaintoutis, A. Fragkos, D. Syvridis: Random number generation from a secure photonic physical unclonable hardware module. (2018). In: E. Gelenbe, P. Campegiani, T. Czachorski, S. Katsikas, I. Komnios, L. Romano, D. Tzovaras (eds.) Recent Cybersecurity Research in Europe: Proceedings of the 2018 ISCIS Security Workshop, Imperial College London. Lecture Notes CCIS No. 821, Springer Verlag

[28]C. Mesaritakis C, M. Akriotou M, A. Kapsalis A, E. Grivas E,C. Chaintoutis C, T. Nikas T, D. Syvridis D. Physical Unclonable function based on a multi-mode optical waveguide. (2018) Sci Rep.; 8:9653. https://doi.org/10.1038/s41598-018-28008-6.

[29] R. A. Hallman, et al. Building Applications with Homomorphic Encryption. (2018). Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2018.

[30]L. Coppolino, S. D'Antonio, L. Romano, L. Sgaglione and M. Staffa (2017). Addressing Security Issues in the eHeatlh Domain Relying on SIEM Solutions. In: Proceedings of the 41st IEEE Annual Computer Software and Applications Conference COMPSAC

[31]A. Theodouli, S. Arakliotis, K. Moschou, K. Votis, & D. Tzovaras. (2018). On the Design of a Blockchain-Based System to Facilitate Healthcare Data Sharing. 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 1374-1379.

[32]L. Castaldo, V.Cinque.: Blockchain based logging for the cross-border exchange of E-health data in Europe. (2018). In: Gelenbe, E., et al. (eds.) Euro-CYBERSEC 2018. CCIS, vol. 821, pp. 46–56. Springer, Cham.

[33]eIDAS website. https://www.eid.as/home/. Accessed on 18 May 2018.

[34]Mariacarla Staffa, Luigi Coppolino, Luigi Sgaglione, Erol Gelenbe, Ioannis Komnios, Evangelos Grivas, Oana Stan, Luigi Castaldo, "KONFIDO: An OpenNCP-Based Secure eHealth Data Exchange System", Euro-CYBERSEC2018: 11-27, Springer Lecture Notes Vol. CCIS 821, Springer Verlag, Berlin, 2018, Open Access, https://link.springer.com/chapter/10.1007%2F978-3-319-95189-8_2

[35]E. Gelenbe, P. Campegiani, T. Czachórski, S. K Katsikas, I. Komnios, L. Romano and D.Tzovaras. Security in Computer and Information Sciences. (2018) First International ISCIS Security Workshop 2018, Euro-CYBERSEC 2018, London, UK, February 26-27, 2018, Revised Selected Papers, Lecture Notes Vol. CCIS 821, Springer Verlag, Berlin, 2018, Open Access, https://link.springer.com/content/pdf/10.1007%2F978-3-319-95189-8.pdf.

[36]P. Natsiavas, J. Rasmussen, M. Voss-Knude, K. Votis, L. Coppolino, P. Campegiani, I. Cano, D. Marí, G. Faiella, F. Clemente, M. Nalin, E. Grivas, O. Stan, E. Gelenbe, J. Dumortier, J. Petersen, D. Tzovaras, L. Romano, I. Komnios and V. Koutkias (2018). Comprehensive user requirements engineering methodology for secure and interoperable health data exchange. BMC Medical Informatics and Decision Making, 18(1):85. https://doi.org/10.1186/s12911-018-0664-0.

[37]Rasmussen J, Natsiavas P, Votis K, et al. Gap analysis for information security in interoperable solutions at a systemic level: the KONFIDO approach. Precision Medicine Powered by pHealth and Connected Health, vol. 66. Singapore: Springer; 2017, IFMBE Proceedings. p. 75–9. https://doi.org/10.1007/978-981-10-7419-6_13.

[38]F. Pecoraro, D. Luzi, M. Cesarelli, F. Clemente (2015) A methodology of healthcare quality measurement: a case study, J. Phys.: Conf. Ser. 588, pp 1-5.

[39]P. Natsiavas. et al. (2018) Identification of Barriers and Facilitators for eHealth Acceptance: The KONFIDO Study. In: Maglaveras N., Chouvarda I., de Carvalho P. (eds) Precision Medicine

Powered by pHealth and Connected Health. IFMBE Proceedings, vol 66. Springer, Singapore. https://doi.org/10.1007/978-981-10-7419-6_14.

Figure

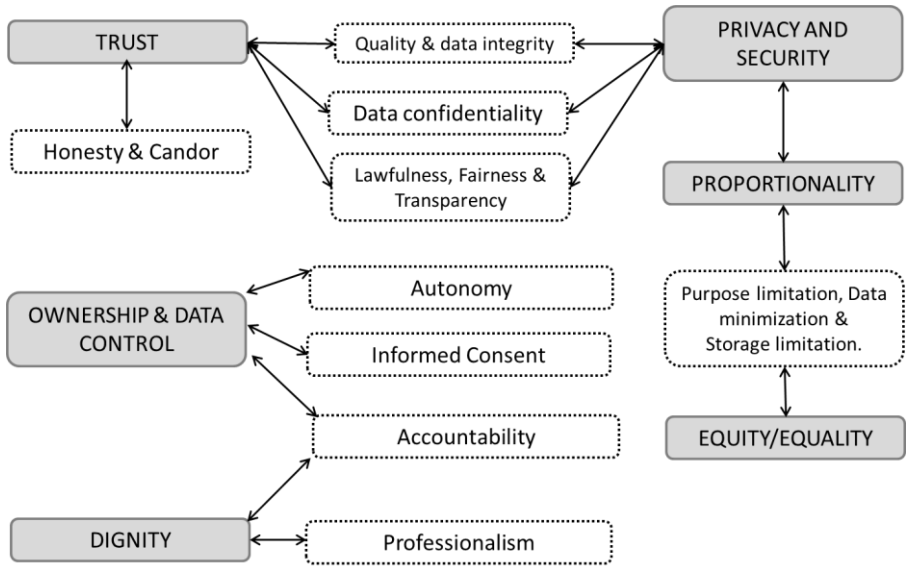


Figure 1: Aggregation of literature findings about ethical principles related to eHealth and cross-border health data exchange (updated from)

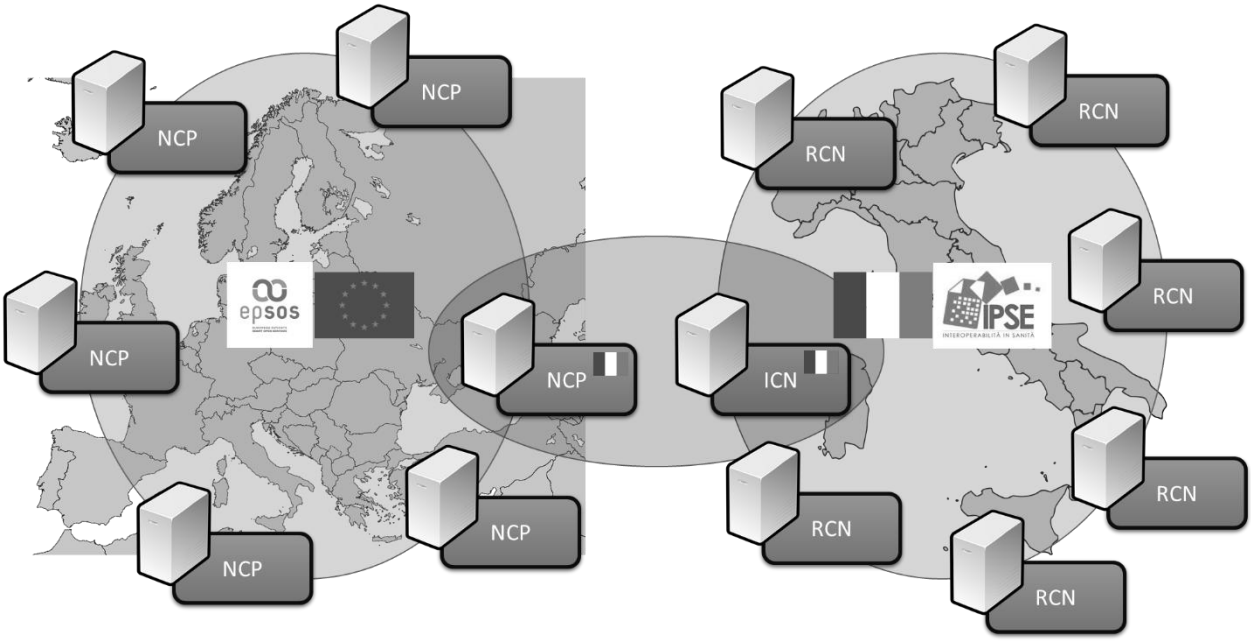


Figure 2: The IPSE infrastructure based on epSOS (new nodes were defined, in particular the Interregional Contact Node (ICN) and Regional Contact Nodes (RCN)) (Adapted from)

[14] G. Faiella G. et al. (2018) Building an Ethical Framework for Cross-Border Applications: The KONFIDO Project. In: Gelenbe E. et al. (eds) Security in Computer and Information Sciences. Euro-CYBERSEC 2018. Communications in Computer and Information Science, vol 821. Springer, Cham.

[19] http://www.arit.it/aree-tematiche/sanita-elettronica/86-il-progetto-ipse.html. Accessed on 2 November 2018

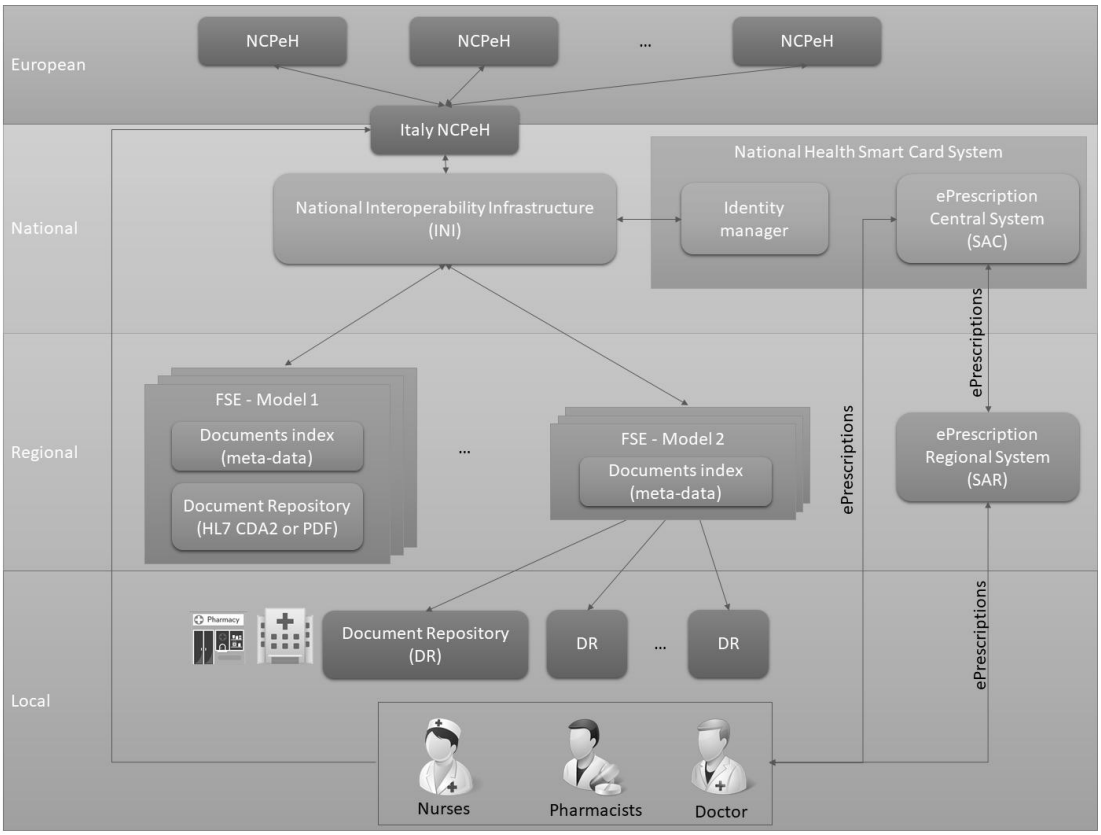


Figure 3: Italian eHealth data Infrastructure

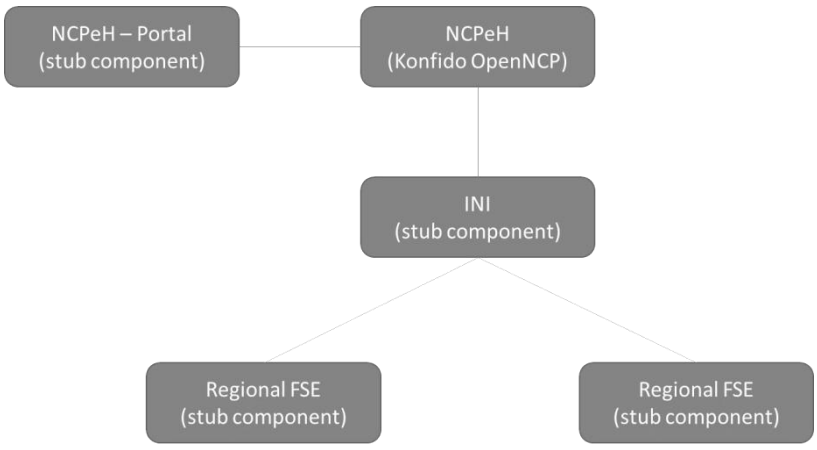


Figure 4: Italian Test-bed for the KONFIDO Pilot

Table
Click here to download Table: Tables.docx

Table 1 – Legal and Organizational Requirements and Barriers

Main Legal & Organizational Requirements	Barriers
Identification of patient	The Member States are not all aligned with eIDAS Regulation and JASeHN agreement [13].
Management of patient consents	Different and complex consent mechanisms among Member States.
Authentication of healthcare provider	The Member States are not all aligned with JASeHN agreement [13].
Management of healthcare professional authorization/certification	The Member States are not all aligned with JASeHN agreement [13].
Enhance interoperability	• Lack of standard electronic health record-system among Member States. • Different implementation of EU regulations among Member States. • Different information workflows among National Infrastructure and healthcare organizations.
Accuracy and integrity of semantic processing.	• Free text content in different languages. • Lack of standard electronic health record-system among Member States. • Different technical solutions for health data digitalization.
Each NCPeh should be compliant with confidentiality, integrity, authenticity, availability, non-repudiation, encryption, logs, audit trails, and other means of data security	The Member States are not all aligned with JASeHN agreement [13].

[13] https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20170509_co06_en.pdf. Accessed on 2 November 2018.

Table 2 - Ethical principles and suggested actions

Ethical Principles	Suggested actions
Trust	• Include appropriate data quality mechanisms and integrity checks. • Data needs to be collected in a standardised way, so that it can be comparable and usable. • Patients must be informed about policies and practices regarding the data exchange that should be provided in a clear and understandable form. • The point of care has to inform the patients regarding potential breaches of data security.
Privacy and Security	• Perform a risk analysis to identify the principle dangers and related remedies. • Prepare an information sheet with details about the security measures.
Proportionality	The data sharing mechanisms should guarantee that the data are not stored longer than necessary in the recipient country and the information is unobstructed when there is an urgent need to obtain data, particularly to prevent loss of life.
Ownership & Data control	The patients have to be informed about the processing of the personal data and they must authorise data manipulation (e.g., provide authorisation for cross-border health data sharing).
Equity/Equality	Cross-border solutions should contribute to equality in healthcare and they should be usable in every EU member country and by each each citizen of the EU.
Dignity	• Cross-border solutions should be designed without ignoring the human aspects and patient rights. The patient is at the centre of the healthcare processes. • Introduce mechanisms that enable a continuous revision of cross-border solutions, according to end-users feedbacks.

Table 3 - Ethical requirements and barriers

Main Ethical Requirements	Barriers
High level of trust and security	European Level: • Lack of harmonization of rules, processes and safeguards. • Lack of official and shared security practices. National/Local level: • Lack of management commitment at local level of point of care. • Lack of the budget to address security aspects by healthcare organizations. • Lack of specific security policies.
Respect of patients' rights: Right to access data, the right to erase and correct data and the right to know who accessed data.	• NCPeH are still in early stages. • Lack of official harmonization of rules.

Table 4: FSE documents according to dPCM n. 178/2015, differentiating the minimum data set and the extended data set [22]

FSE Documents		
Minimum Dataset	**Other Documents**	
Identification and administrative data of the patient	Prescriptions	Hospital care
Medical reports	Reservations	Medical certificates
Emergency reports	Medical records	Patient's personal notebook
Discharge letters	Health checks	Continuity of care
Patient summary	Home care	Self-certifications
Pharmaceutical dossier	Diagnosis and treatment plans	Participating in clinical trials
Choice regarding the donation of organs and tissue	Semi-residential care	Exemptions
	Dispensing medications	Prosthetic assistance
	Vaccinations	Data to support the activities of telemonitoring
	Outpatient care	Data to support the activities of the integrated management of diagnostic and therapeutic
	Emergency care	Other relevant documents

[22] Decree of the President of the Council of Ministers - dPCM n. 178/2015

Table 5 – Legal, Organizational and Ethical Requirements and solutions that will be implemented in Italy at European and National/Regional Level

Main Legal, Organizational & Ethical Requirements (Table 1)	Italian European level solutions	Italian National/Regional solutions
Identification of patient	The Italian infrastructure will provide an eIDAS compliant system for Italian patient abroad. It will recover foreign patients identities from the other countries eIDAS systems.	The patient is identified through a national health smartcard system, with SPID identification system.
Management of patient consents	The same national system is used also at international level	The consent management process is defined at National level despite the fragmentation of the regional healthcare systems. Every region will collect consent for its citizens and it will provided to the other Regions upon request.
Identification of healthcare provider	The same interregional system will be used at international level	The National smart card system defined clear procedure and roles for the identification and authorization of the healthcare providers.
Management of healthcare professional authorization/certification	In the international context, when Italy is operating as country B, they will authenticate with SPID anyway, but consulted directly by the OpenNCP node instead of the usual regional FSE.	At regional level, each healthcare professional will authenticate using the same SPID system used by the patients. They are then authorized at regional level by the healthcare providers.
Enhance interoperability	Interoperability toward European countries will be ensured trough the implementation of OpenNCP. The	In Italy, the interoperability is defined at National level and implemented trough the Italian interoperability

	"Deployment of Generic Cross Border eHealth Services in Italy" initiative has the roadmap to implement it within 2020. Nations will exchange patient summary and ePrescription only.	infrastructure (INI). 11 Regions already adhered to INI and others have plans to join it in the future. Regions will be able to exchange the full FSE.
Accuracy and integrity of semantic processing.	This will be ensured by the deployment of the NCPeH.	The IPSE project proposed to test the semantic interoperability building block of epSOS also at National level: even if the language is the same, there are different regional names and definitions which must be harmonized.
Each NCPeh should be compliant with confidentiality, integrity, authenticity, availability, non-repudiation, encryption, logs, audit trails, and other means of data security	This will be ensured by the deployment of the NCPeH.	The IPSE project claimed that security and auditing mechanisms defined by epSOS will be exploited also at National level.
High level of trust and security	Adoption of the eHealth Network guidelines in the implementation of the NCPeH.	Definition of the common framework of the National FSE and the INI.
Respect of patients' rights: **right to access data, the right to erase and correct data and the right to know who accessed data.**	Adoption of the eHealth Network guidelines in the implementation of the NCPeH.	Clear consent management and consent revoke processes are defined at National level and implemented at Regional level.

Table 6 - – Legal, Organizational and Ethical Requirements and solutions that will be implemented in the Italian Pilot

Main Legal, Organizational & Ethical Requirements (Table 1)	Italian pilot solutions
Identification of patient	The Italian pilot will test an enhanced customized eIDAS system.
Management of patient consents	The Italian pilot will implement a stub virtual process for the consent management in line with the actual National system.
Identification of healthcare provider	In the Italian pilot the identification of healthcare providers is not a main focus for validating Konfido technologies, thus two ad hoc healthcare providers will be preconfigured in the Italian testbed.
Management of healthcare professional authorization/certification	In the Italian pilot, the same stub for digital identity used for the patients will be used also for healthcare professionals. As for the healthcare providers, they will be pre-configured in the testbed.
Enhance interoperability	Enhance interoperability will be tested in the pilots using Konfido solutions both at NCP level and regional level.
Accuracy and integrity of semantic processing	The pilot will leverage on the OpenNCP functionalities (like OpenNCP transformation service) secured by Konfido (laveraging on the trusted executing environment).
Each NCPeh should be compliant with confidentiality, integrity, authenticity, availability, non-repudiation, encryption, logs, audit trails, and other means of data security	This is one of the main pilot focus, leveraging on the innovations provided by Konfido, both at national and international level, and the added value will be validated.
High level of trust and security	The pilot will test the security enhancements proposed by Konfido both at National and International level.

Respect of patients' rights: **Right to access data, the right to erase and correct data and the right to know who accessed data.**	As patients are defined in Konfido as beneficiaries of the innovation, but not as main users, the respect of their rights will be considered implicit and will not be tested.

Table 7: Preliminary criteria for pilot validation

Validation Criterion ID	Criterion	Comment
VC 1	Percentage of modules successfully integrated	This criterion would highlight the efficacy of KONFIDO solution components.
VC 2	Percentage of misuse cases handled better compared to plain OpenNCP	This criterion would depict the contribution of KONFIDO solution in the specific target misuse cases.
VC 3	Percentage of user goals satisfied	The finally deployed KONFIDO solution would be compared with the abstract user goals identified in the overall KONFIDO user requirements process, in order to assess the contribution of the KONFIDO solution with the overall end-user needs.
VC 4	Technical validation criteria based on standards and widely accepted security best practices (NIST, ISO 27K etc.)	A detailed list of relevant validation criteria will be elaborated based on information from widely accepted IT security standards and best practices (e.g. ISO 27000 and NIST).
VC 5	User acceptance criteria	The KONFIDO consortium will actively elaborate on available options (e.g. usability testing, questionnaires, interviews etc.), in order to identify the appropriate solution given the project's overall pilot plan, the available time as well as financial constraints.