Legal aspects regarding the use and integration of electronic medical records for epidemiological purposes with focus on the Italian situation

Antonietta Stendardo[1, 2], Francesca Preite[3, 4], Rosaria Gesuita[5], Simona Villani[1], Antonella Zambon[6] and the SISMEC "Observational Studies" working group

ABSTRACT

The "Observational Studies" working group of the Italian Association of Medical Statistics and Clinical Epidemiology (SISMEC) has undertaken to study the impact of recent healthcare sector regulations on the legal and organisational aspects of managing all EMR databases with emphasis on Legislative Decree No. 196/2003 (the Italian Personal Data Protection Law).

This paper examines six issues relating to theirs legal implications. The first section, "Confidentiality", provides definitions and the regulatory context for the terms "confidentiality" and "personal data". In the second, "Nature of data held in electronic medical record archives", we discuss the problem of sensitive data and procedures to make the identification code anonymous. In "Data ownership" we highlight the difference between the data controller and the database controller. The fourth section, "Conditions for processing", discusses problems associated with using research data from one study in other investigations. In the fifth, "Patient consent", we address the problems related to patient consent. Finally in "Penalties" we outline the main civil and criminal liability issues applied in case of non-compliance with the provisions of the Personal Data Protection Code. Where possible, we provide suggestions on how to comply with the legal requirements of managing medical record archives in order to make it easier for researchers to remain in compliance with the relevant provisions.

Key words: Legal aspects; Database; Epidemiology

(1) Department of Public Health, Experimental and Forensic Medicine, Unit of Biostatistics and Clinical epidemiology, University of Pavia, Pavia, Italy

(2) Senior partner of Legal Study Nesci-Stendardo, Messina, Italy

(3) Senior partner of Legal Study Miari-Preite, Reggio Emilia, Italy

(4) MediData S.r.l., Modena, Italy

(5) Centre of Epidemiology, Biostatistics and medical Information Technology, Polytechnic University of Marche, Ancona, Italy

(6) Department of Statistics and Quantitative Methods, Unit of Biostatistics, Epidemiology and Public Health, University of Milano-Bicocca, Milan, Italy

CORRESPONDING AUTHOR: *Antonietta Stendardo, Department of Public Health, Experimental and Forensic Medicine, Unit of Biostatistics and Clinical epidemiology, University of Pavia, Pavia, Italy. Tel. +39 0382 987540, Fax +39 0382 987183. e-mail: avv.antoniettastendardo@virgilio.it*

DOI: ***10.2427/8971***

INTRODUCTION

In Italy, there is a large number of medical databases that collect individual data with the purpose of carrying out epidemiological studies. For instance many large cohorts have been recruited over the past 10-20 years in studies investigating cardiovascular risk factors; studies like the MONICA project (Multinational MONItoring of trends and determinants in CArdiovascular disease) and the PAMELA project (Pressioni Arteriose Monitorate E Loro Associazioni - monitored blood pressure and associations) have gathered information on more than 20 000 individuals.

At the same time, over the past 10 years automated medical information databases, originally created for service-related organisational purposes and to monitor health expenditure and resources (e.g. the pharmaceutical prescription archive, the hospital discharge records archive), have also been used for epidemiological investigations. Despite being designed, implemented and used for purposes other than standard epidemiological studies, these databases have proved useful in setting up registration and monitoring systems for adverse health events, and in running descriptive and analytical epidemiological investigations. Administrative databases offer low-cost information, generally regarding all health services provided in a given area of authority; more importantly, unlike the other systems which monitor and assess treatment quality, they do not require investment of further resources for the operators and services involved.

Clearly, this approach also entails problems and drawbacks. The main problem is the need to check to what extent an information, flow programmed and created to meet requirements substantially of administrative nature in a service management context, can provide the degree of detail and comprehensiveness needed to conduct epidemiological research. Secondly, the need to run joint queries on these archives presupposes that it should be possible to locate in each archive and across archives all health services received by an individual by means of a record linkage using a unique identification code.

Whatever the type of electronic medical record (EMR) archive, i.e. whether the data was collected for administrative or for specific purposes, a major issue that must be addressed is how to guarantee data confidentiality and patient anonymity, since individual information is often accessed without the patient concerned being involved. This issue is particularly important when EMR deriving from different sources need to be integrated.

The legislation governing these issues is extremely complex and fragmented and has already been the subject of specific changes. Nevertheless, the legal aspects of managing and using the medical records and data held in these databases often involve extremely complex operating solutions.

CONFIDENTIALITY

Definition and regulatory framework

For Louis Brandeis, an Associate Justice to the US Supreme Court, privacy was the right to one's own personal information and private life, and the right to be let alone. Louis Brandeis and Samuel Warren were probably the first to draw up a "privacy" law [1]. Over time the concept has changed to encompass facts predominantly related to a subject's personal sphere, whereas confidentiality pertains to the treatment of information. However, Italian data protection law is referred to as "Privacy" law.

In Italy, the culture of "data privacy" is embedded in the Constitution. Its constitutional basis is to be found in Articles 14, 15 and 21, and concern the domicile, the freedom and secrecy of personal correspondence, and freedom of thought. In addition, Article 2 of the Italian Constitution mentions privacy as one of "man's inviolable rights".

In Italian legislation "privacy" initially referred to aspects of an individual's private life, but over the past 10-20 years it has evolved to encompass a wider definition. It currently means "control over oneself and power to determine one's own fate " [2]. Privacy is usually construed as the right to be let alone; recognition of this right is a means to safeguard our liberty and our deepest aspirations.

The rights of an individual are recognised in the UNIVERSAL DECLARATION OF HUMAN RIGHTS and in the EUROPEAN CONVENTION ON HUMAN RIGHTS.

The main European sources of legislation are set out in the DIRECTIVE of the EUROPEAN

PARLIAMENT and COUNCIL of 24 October 1995, 95/46/EC [3].

Current personal data protection law in Italy is set forth in Legislative Decree No. 196 of 30 June 2003, which repealed Law No. 675 of 1996, known as the "Privacy Law".

Prior to the "Privacy Law", the main source of legislation for such issues was the Court of Cassation. After initially denying the existence of a right to "privacy" in 1956 (ruling no. 4487), in 1975 the Court defined it by reference to Article 2 of the Italian Constitution as the right to "safeguard strictly personal and family-related situations which are of no socially significant interest to third parties, even when they occur outside of the home" (ruling no. 2199).

The Personal Data Protection Code in force in Italy since 1 January 2004, introduced by Legislative Decree No. 196 of 30 June 2003 [4], was enacted as a result of the third extension the courts granted the government under Law No. 676/1996, in order to integrate, rectify and complete the original provisions contained in Law No. 675 of 31 December 1996, which had transposed and updated Directive 95/46/EC.

With respect to Law No. 675/1996, which consisted of only 45 sections divided into 10 chapters, Legislative Decree No. 196/2003 comprises 186 sections divided into three parts:

1. the first part establishes the general principles and scope of the legislation;
2. the second part covers special aspects of data protection;
3. the third part addresses the failure to comply with the law or its incorrect application.

Legislative Decree No. 196/2003 is also integrated by three addenda containing the codes of conduct and professional practice, minimum security measures and non-occasional handling of personal data for administering justice or for police use.

NATURE OF DATA HELD IN ELECTRONIC MEDICAL ARCHIVES

The Italian Personal Data Protection Code classifies data into four categories as follows:

- *Sensitive data:* data disclosing information on race or ethnic origin; religious, philosophical or other beliefs; political opinions, membership of political parties, trade unions, associations or organisations of a religious, philosophical, political or trade unionist character; as well as personal data disclosing information on the health status and sexual life of an individual.
- *Semi-sensitive data:* information whose processing could damage the individual concerned (e.g. data relating to individuals suspected of fraud or regarding financial situations).
- *Ordinary data:* any information, including name, surname, VAT number, tax code, address, phone number or driving licence number, which can be used to identify a physical or legal person, bodies and associations included.
- *Judicial data:* information disclosing measures concerning the criminal record office, the list of fines applied as a consequence of administrative offences committed, and any outstanding charges.

Both sensitive and ordinary data is considered to be part of the more general category called "personal data".

The concept of "personal data" includes all information, details or elements that can effectively add to the knowledge about an identified or identifiable individual [5].

EMR archives (patient records, prescriptions, hospital discharge files, etc.) do not contain exclusively sensitive data.

For instance, a patient's medical record saved in a hospital's electronic archive contains information regarding the patient's profession, mobile phone number, and whether he/she has siblings or children, all information which is not sensitive.

Genetic data is considered to be sensitive, and is also referred to as "super-sensitive data" due to the special treatment reserved to it by the Privacy Authority. Genetic data is also held in EMR archives.

At the other end of the spectrum from sensitive personal data is "anonymous data" which, under Italian personal data protection regulations, concerns a physical person who cannot be identified by the data controller or anyone else using all the methods which may reasonably be adopted by the data officer or anyone else involved in data processing, to identify the individual.

Anonymous data originally relates to one or more identifiable individuals who, after data anonymisation (i.e. a type of processing that

is usually achieved by a statistical method), can no longer be identified; for all intents and purposes such data thus becomes anonymous.

This point is often misinterpreted, and it should be emphasised here that it would be incorrect to claim that data not associated with a name is anonymous and therefore not personal; indeed, information may not have an associated name but can still be personal if it contains elements which would allow a person to be identified (a patient code, date of birth, age, sex, height for example).

The distinction between anonymous data and personal data is critical, because the former data can be freely shared and is not subject to any restrictions or to the provisions of privacy law.

Since the Italian Personal Data Protection Code deals exclusively with "personal data" and its sharing, the distinction between sensitive and non-sensitive data does not apply when anonymous data is concerned.

The legislation examined in this document provides no specific restrictions for the handling of anonymous data: the data subject's consent is not required nor notification needed to the Privacy Authority. For example, researchers conducting a clinical study must abide by the provisions of data protection legislation and acquire patient data only with their consent. Once this data has been aggregated and used to generate anonymous statistical reports, the reports can be freely circulated and no further personal data protection restrictions apply, because once the data has been made anonymous, it has ceased to be personal.

An additional category often used in clinical research, is "aggregate data". This kind of data is originally personal and is then processed and pooled with the data of other subjects; if there are no associated identifiers (not necessarily names), this data is anonymous and can therefore be freely shared.

An example of anonymous data, i.e. information collected and examined for statistical purposes and subject to statistical confidentiality, would be the official statistics of the Italian National Institute of Statistics (ISTAT).

Learning about the habits of a group of individuals through a series of percentages gives no indication of their identity.

The personal data and information collected during an interview as part of a National Statistics Program survey is protected by statistical confidentiality and subject to personal data protection provisions.

The data collected and examined can be used in subsequent analyses for purely statistical purposes, by operators and officers of the national statistics system.

The data can be used for scientific research purposes in line with the conditions and procedures laid down in Section 7 of the Code of Conduct and Professional Practice that applies to the handling of personal data within the national statistics system.

This data will be distributed in aggregate form so that the subjects to whom it refers or who originally supplied it cannot be identified.

The Data Controller of data used for official statistical purposes is ISTAT, irrespective of the body that actually collected the data.

The Italian National Institute of Statistics is obliged by law to respect statistical confidentiality governed by Section 9 of Legislative Decree No. 322 of 6 September 1989 as amended (Subsections 1 and 2 of Section 9 were amended by Section 12 of Legislative Decree No. 281 of 30 July 1999, effective 1 October 1999).

Statistical confidentiality has two purposes:

- to protect the public interest in maintaining a healthy production of official statistics;
- to protect the subjects involved, ensuring that their private information is not disclosed.

Statistical confidentiality is the foundation of the trust between public institutions generating statistics and respondents (citizens, families, businesses, institutions, etc.). Official statistical bodies adopt this principle as a rule of conduct, refusing to disclose or release to anyone any kind of recognisable individual information.

Being public entities, the operators and officers of the national statistics system are obliged not only to abide by statistical confidentiality but also by official confidentiality as required under Section 8 of Legislative Decree No. 322 of 1989.

Statistical confidentiality must therefore not be confused with official confidentiality or professional confidentiality.

Official confidentiality is required of public officials and individuals charged with a public service, who are obliged to keep confidential any information acquired by way of their positions or the services they perform; this may be required by law, order by a public authority, or custom

or may be due to the nature of the information, which must not be disclosed to other parties.

Professional confidentiality applies to lawyers, doctors, accountants, pharmacists and all healthcare professionals; in other words, the professional subjects that an individual must interact with to protect his/her personal interests and health, disclosing confidential or intimate information in the process.

Let us now turn to the information contained in a medical record.

The unlawful disclosure of the contents of an individual's medical record could lead to criminal charges for breach of professional confidentiality (Section 622, Italian Criminal Code) or official confidentiality (Section 326, Italian Criminal Code) and a formal reprimand from the relevant professional register. Another example is the case of medical students and trainee doctors, who are bound by professional confidentiality but not by official confidentiality, given that they are not part of the university hospital organisation.

DATA OWNERSHIP

To establish who is the owner of the information held in a database, a distinction must first be drawn between the "data controller" and the individual who actually owns the database.

In data protection legislation, "data controller" means any physical or legal person or administrative or other body, association or organisation entitled, either alone or with other persons, to determine the purposes, manner and means whereby personal data is processed, including the adoption of data security measures (Section 28, Personal Data Protection Code).

The physical or legal person who owns the actual database is a completely different entity; this will be whoever has created the database or later acquires the right to use it (for economic or other purposes).

These two entities are not always one and the same.

Being owner of the database involves specific legal obligations which must be observed in the acquisition and conservation of all data. For example:

- data must be acquired with the subject's consent;
- data can only be used for the purposes reported in the privacy statement;
- data can only be disclosed to third parties with the subject's consent;
- database management must adopt minimum security measures;
- data subjects must be informed of what data is held about them;
- data must be deleted if so requested by the data subject (although the Privacy Authority may allow clinical researchers to keep any data already acquired). In other words, it would be correct to state that the database belongs to the individual / body that created it, but the personal data contained within remains the property of the individuals it refers to, who retain all relevant rights, including the right to withdraw consent to the processing of their personal data (Section 7, Personal Data Protection Code).

However the issue is much debated and there is no easy solution from a legal point of view.

A Missouri District Court in the United States passed a ruling addressing the problem. Ownership of a number of biological samples, contained in a bio-bank stored in Washington University, was attributed to the university and not to the physical subjects who had provided them. The court thereby established that the samples are a distinct entity, separate from the individual providing them and who, by giving their written consent that their samples could be used, also waived title to them.

This kind of ruling is still alien to Italian law.

Of interest in this regard is the recent debate over the intellectual property of databases.

A collection of works, data or other independent elements which are systematically or methodically arranged and individually accessible using electronic or other means (i.e. a database) constitutes an intellectual creation and is therefore protected by law. Copyright protection of databases does not extend to their contents, and any rights to the contents remain unaltered [7]. Therefore, a subject may be the owner of a database but have no power over the individual data contained in it. This applies to personal data; when data becomes anonymous or is aggregated, as explained later, the individual supplying the data no longer has any title to it.

So while it may be clear that a database benefits from the protection extended to any intellectual work, the nature of the rights concerned is still debated. These rights are similar to copyright but singular enough to warrant classification as a *sui generis* right according to some authoritative experts.

CONDITIONS FOR PROCESSING

Subsequent use of information collected for a specific research project

Data protection legislation lays down specific requirements for the safekeeping of personal data stored digitally, as hard copy or by any other ways.

It also provides clear rules regarding the destruction of supports containing sensitive data when it has to be deleted, for example when a project has been completed and the conservation period for the associated data has expired, which depends on the purposes stated at the time of collection.

Personal Data Protection Code, Schedule B, Para 22 "If removable supports containing sensitive or judicial data are not used, they must be destroyed or made unusable; otherwise they can be reused by other bodies, not authorised to handle the data originally stored on the support, provided that said data is illegible and technically impossible to reconstruct".

The wording of this provision shows that the Privacy Authority intended to ensure that once the data has been used for the intended purpose, it must be deleted.

In any case, data and biological samples provided by individuals taking part in experiments and observational studies must be conserved only as long as is necessary to achieve the purposes for which they were collected and processed (Section 11, Subsection 1, letter e, Personal Data Protection Code).

A further provision requires that the purpose for which data is handled be clearly explained on the consent form that the patient signs when deciding to take part in a research project.

The current Privacy Authority Authorisation to process genetic data [8] contains the following provision: "Genetic data may only be handled and biological samples used for the purposes ..... stated in the informed consent provided by the subject in advance and in writing".

The Privacy Authority makes similar provisions for medical data [9]: "…the strict relevance, non-superfluous and necessary nature of the data in relation to the relationship, service or task being performed, to be established or terminated, must constantly be monitored, and regular checks established if necessary. This requirement shall also apply when the information has been provided spontaneously by the data subject. Any superfluous, irrelevant or unnecessary data must not be handled, other than for the purpose of conservation".

Only in given cases can data collected for projects or for specific therapeutic purposes be reused without the data subject having to sign a new consent form.

Storing data and reusing it in different research projects and statistical surveys than those for which the data subject originally gave his/her informed consent is only permitted for scientific and statistical purposes directly connected with the original ones (Section 8.1; Auth. Privacy Authority for genetic data processing cited above).

It can thus be inferred from the Privacy Authority's provision that data legally stored in electronic medical archives can only be reused for a scientific research project or statistical study that is directly connected with the one for which consent was obtained.

Given this provision, medical centres acquiring and processing personal data for therapeutic purposes should consider obtaining express patient consent also for processing of said data by the same centre for statistical and scientific purposes.

Sharing data outside the medical centre (to university centres for example) without the patient's express consent (except for the situations detailed below) and for purposes that have not been clearly defined, raises many doubts in terms of regulatory compliance.

Clearly data that has been anonymised and aggregated, as mentioned earlier, can be shared freely.

Use of patient medical data without patient consent

Section 110 of the Code of Conduct and Professional Practice for the handling of personal data for statistical and scientific purposes allows said data to be used in epidemiological research or in scientific-statistical studies without the consent of the data subject only in presence of ethical or methodological grounds, or when organisational restrictions make it impossible to inform the data subjects, provided that the research programme has been approved by the relevant ethics committee and data processing authorisation has been received from the Privacy Authority. Only when these conditions have been met the data held in medical archives can be reused in a research project without having to re-obtain the patient's consent.

It should be underlined that the Privacy Authority's authorisation is subject to an *ad hoc*,

fully documented application which is examined by the relevant offices on payment of a fee; approval (or refusal) is notified within 45 days of the application being received. Since this period starts from the time the further documentation or clarifications usually solicited by the office are provided, and given that all applications remain pending during the month of August, the process usually takes much longer.

Following a period of public consultation, on March 1st 2012 the Privacy Authority issued a general authorisation to use medical data (excluding genetic data) for scientific purposes. The permission was initially granted for a limited period (up to 31 December 2012) and now up to 31 December 2013, but it is expected to be renewed. The authorisation regards exclusively retrospective observational clinical studies (including studies based on administrative databases) and enables data controllers to proceed without patient consent, provided that:

- the appropriate ethics committee has issued its approval,
- there are ethical grounds advising against informing patients of the trial (because it may cause them material or psychological harm), or
- there are organisational reasons making it impossible to inform patients who are found to be deceased or untraceable after substantial research (in this case the exemption applies to deceased or untraceable patients only).

If the retrospective study meets the conditions laid down in the aforementioned authorisation, it can go ahead without patient consent (only untraceable patients when the grounds are organisational); otherwise (e.g. for retrospective studies using genetic data, where it is impossible to inform the data subjects for methodological reasons), in order to carry out the study without patient consent, the authorisation of the Privacy Authority must be sought as described above.

PATIENT CONSENT

Declaration of Helsinki (June 1964)

In biomedical research, a fundamental distinction must be drawn between medical research carried out primarily for diagnostic and therapeutic purposes and medical research carried out purely for scientific purposes and with no direct diagnostic or therapeutic implications for the subject.

In all studies involving HUMANS, each potential participant should be informed of the purposes, methods, expected benefits and potential risks of the study and of any adverse events which could result. They should also be informed that they are free to leave the study and withdraw their consent at any time. After adequate information has been provided, the doctor should ask for their free consent, preferably in writing.

The Declaration of Helsinki is the main reference for patient consent issues in medical research.

Later laws on clinical research cover exclusively experimental studies and nearly always exclude observational studies (with the exception of the Guidelines of the Italian Medicines Agency - AIFA - of 20 March 2008 which however are "secondary sources of legislation").

Given the long-standing lack of specific legislation on observational studies the principles governing experimental research have been applied to this type of research by analogy.

In clinical trials, all sources stress that subjects may not be included in the study if they have not been adequately informed and have not given their valid consent.

Speaking non technically, patient consent can be defined as the document governing the researcher-patient relationship and setting its legal boundaries.

Only what the patient has consented to can be done; whatever the patient has refused to agree to or has not given consent to (because the question was not asked) cannot be done.

It is now important to take a closer look at observational studies.

Observational studies do not entail different procedures from those envisaged in routine clinical practice.

Since current law on experimental studies is not completely adequate to observational studies, and since patients do not randomly undergo any procedures in the last kind of studies, and also taking into account the content of the consent form asked to sign in observational studies, it can be concluded that the consent to take part in an observational study equates with the consent to the processing of personal data. Despite this, patients are often asked to sign two different forms.

Indeed, patients agree that their medical and non-medical data (which is already contained in their records) can be used and agree to provide additional details in the future, undertaking to undergo medical examinations (which we could call "meetings"). The form commonly known as the "clinical trial patient form" is essentially a statement of the nature, purpose and method of personal data processing, basically the same data that must be provided in a data privacy statement.

Despite this, the major source of law for observational studies (the 2008 AIFA Guidelines) fails to lay down specific provisions on this point, stating instead that the patient informed consent form and the personal data consent form must both be presented to the ethics committee, thereby emphasising the difference between two issues which for the patient in fact coincide.

For example, could a patient agree to take part in a study but not allow his/her personal data to be processed? The answer, clearly, is no: not because this is what the law lays down, but because the two consents are actually the same psychological issue for the patient.

Nevertheless, compliance with AIFA Guidelines and the Declaration of Helsinki requires the patients to CONSENT to taking part in the study.

This consent must be given IN WRITING by an individual who is LEGALLY ABLE (subjects who are legally unable to give valid consent would be minors, incompetent adults, all individuals who are visibly mentally incompetent or incapacitated, either temporarily or permanently) after they have been ADEQUATELY INFORMED (the word adequacy introduces a degree of discretion to be assessed on a case-by-case basis).

It can therefore be inferred that patient consent must be preceded by provision of a STATEMENT, which must:

- be read and signed before patient inclusion in the study, therefore prior to any data being collected;
- be clear and transparent;
- be comprehensive as to the purposes, methods, benefits and potential risks (which requires careful planning of all potential stages and developments in the research programme);
- be clear as to the patient's right to withhold consent and the possibility, method and consequences of withdrawing it;
- contain all other useful and essential information depending on the specific nature of the study.

Researchers may not do anything that does not appear in the patient form and for which consent has not been requested.

It follows that the consent only applies to the specific study for which it was requested.

Example: a patient has agreed to take part in the "Alfa" study on the consequences of a blood disorder and has therefore agreed that his/her blood sample may be analysed for the purposes of the study and that lifestyle and medical data can be collected.

If a researcher working for the same pharmaceutical company or hospital decides at a later date to use the data collected in the Alfa study in a new "Beta" study, again looking at blood disorders, a new patient consent form must be signed. This is needed to allow the patient to assess the purposes/procedures/specific risks of the new study and give his/her consent if they think they are acceptable.

This rather strict approach is relaxed in AIFA Guidelines, which specify that when there is no direct contact with the patient, the consent form does not have to be attached to the application (or more correctly, the notification) sent to the ethics committee; so it would appear that patient consent is not necessary when no direct contact is expected with the patient.

However, this discipline needs to be better coordinated with Privacy Authority provisions; in retrospective observational studies the requirement for patient consent is waived in presence of a number of additional conditions (the motivation why it is, within reason, impossible to obtain consent, and the granting of the authorisation of the Privacy Authority).

It follows that studies not involving direct patient contact can result in contradictory situations in which researchers can carry out their investigation without the informed consent form for the study but still need to ask patients to sign the personal data consent form.

This is another reason for combining the two forms also from the legal viewpoint.

The penalty for failing to obtain patient consent or for inappropriate or inadequate consent, is that any data collected may not be used; moreover, criminal charges or damages may apply.

Measures required to comply with data protection legislation

As discussed before, the person initiating an activity in which personal data is handled will be the "data controller" under privacy law if he/she is the person responsible for deciding for what purposes and in what way any data collected will be used. The data controller must abide by the provisions of Legislative Decree No. 196/2003 which dictates a number of procedures to safeguard individuals to whom the data refer (the "data subjects"). The "data officer" is the physical or legal person, public administration, body or other agency that processes personal data on the controller's behalf, and the "data processors" are the individuals authorised by the data controller or data officer to carry out processing operations. The data controller's main obligations are governed by several provisions of Legislative Decree No. 196/2003; these include the obligations to:

- notify the Privacy Authority of data processing described in Section 37, Subsections 1 and 2 (in the cases specified in the legislation), attaching the authorisation request when sensitive data is involved and the request to transfer data outside of the EU, as applicable (Section 37, Subsection 3);
- adopt the DPS (data security policy document); this only applies to data controllers handling sensitive data in digital format;
- define data collection methods and the requisites of data to be collected (Sections 11 and 13);
- inform data subjects (using the personal data consent form, regulated by Section 13);
- obtain the consent of the data subject (Section 23), using a more detailed statement when genetic data is involved;
- adopt appropriate and minimum security measures (Section 31 et seq. and Schedule B, as well as general authorisations and guidelines for data processing in experimental clinical studies).
- comply with all legal requirements applicable to the data controller's structure (Section 29);
- comply with rules applicable when data is no longer handled and/or has been made over (Section 16);
- pay compensation for any damage resulting from the processing of personal data, including non-pecuniary damage (Section 15).

The obligations of public authorities and bodies

Public authorities and bodies are legal persons having a legal personality (legal capacity and capacity to act).

Their public nature involves an obligation to protect the general public interest.

The Personal Data Protection Code states that unlike physicians and healthcare providers public authorities and bodies are not required to obtain consent to collect and process personal data. In fact they are permitted to carry out these activities in parallel with their institutional functions even where there is no directly applicable legislation or regulations making express provision for this.

More specifically, consent is not required in the following cases:

a) to process data in order to meet the provisions of European laws/regulations/guidelines;
b) to process data to fulfil a contract that the data subject is party to or, before completion of the contract, to meet specific requests of the data subject;
c) to process data obtained from public registers, lists or records in the public domain;
d) to process data to safeguard the life/safety of a third party;
e) to process data when required as part of some preliminary investigations or to protect or defend a right in court proceedings;
f) to process data in order to pursue a legitimate interest of the data subject or of the third party recipient of the data, in specific cases identified by the Privacy Authority;
g) when non-profit associations, bodies and organisations, including non-recognised ones, process the data of their members or of subjects with whom they are in regular contact;
h) to process data for the purposes of scientific, statistical or historical archives, in accordance with the relevant codes of conduct and professional practice.

Notably, based on the provisions of the Personal Data Protection Code, public authorities and bodies are responsible for bringing data processing into line with the institutional function actually performed.

Public authorities and bodies can therefore process personal data without obtaining the subject's consent, only in the aforementioned cases. In contrast, the patient statement must always be provided, in so much as there are no exceptions specifically exempting the public administration.

Public authorities and bodies must also introduce specific regulatory procedures to guarantee the basic rights recognised by law.

Unlike public authorities and bodies, private organisations and public entities (such as universities, chambers of commerce, professional registers) can process personal data only with the prior express consent of the data subject, unless any of the conditions for which consent is not legally necessary are met (Sections 23 and 24 of the Personal Data Protection Code).

Public health authorities are subject to the provisions of Section 76 of the Personal Data Protection Code, which waive the requirement to obtain the Privacy Authority's authorisation, with the data subject's consent, when processing data disclosing details of a subject's health, in relation to data and operations that are essential to protect the subject's safety and health.

Public authorities and bodies are also required to introduce "security measures" to guarantee the security of their data processing operations.

Obligation to request the Privacy Authority's authorisation to process sensitive and genetic data

Legislation regarding the processing of sensitive data is much stricter.

In addition to the provisions discussed above, Section 26 of Legislative Decree No. 196/2003 also requires that permission be requested from the Privacy Authority to use the data.

It should be emphasised that there is a significant difference between notifying and applying for an authorisation by the Privacy Authority.

Notification refers to a number of details sent to the Privacy Authority to allow its monitoring of a given body or institution more effectively and ensure it is following legal procedure; authorisation on the other hand, refers to a condition required for data processing by the data controller.

As expressly stated in Section 26, Subsection 2, the Privacy Authority must respond within 45 days of receiving the request.

Failure to receive the authorisation (i.e. if no response is received within that time) means that it has not been granted.

In granting an authorisation, the Privacy Authority may also request specific measures and actions from the data controller in order to protect the data subject.

The Personal Data Protection Code makes very strict provisions for sensitive data and more specifically medical data. Nevertheless, Section 26, Subsection 3 also envisages a number of exceptions (such as data disclosing membership of religious groups or trade unions) as well as a tool that is often used by the Privacy Authority.

This tool is the so-called "general authorisation", which allows subjects, who find themselves in specific circumstances described by the law, to be granted the Privacy Authority's preventive authorisation to process sensitive data, even though it has not been expressly requested.

This is envisaged under Section 40 of Legislative Decree No. 196/2003 which reads "the provisions of this code prescribing an authorisation from the Privacy Authority are also met by the issue of authorisations for specific categories of data controller and data processing, published in the Official Journal of the Republic of Italy".

The Authority has been exercising this power since 1997, issuing several authorisations which have been repeatedly extended, most recently on 24 June 2011 (authorisation to process genetic data and authorisation to process data disclosing details of a subject's health and sexual life).

The full text of these authorisations can be read on the Authority's website at http://www.garanteprivacy.it

Security measures required for data processing

The consolidated Personal Data Protection Code addresses security in Title V, Part I.

Security measures are the technical precautions that must be taken to protect personal data undergoing processing.

Two measures in particular are relevant to the present discussion: "minimum" and "appropriate" security measures.

Minimum security measures are referred to in general in Section 33 et seq. of the consolidated Data Protection Code, then explained in more detail in the technical specifications outlined in Schedule B to the Personal Data Protection Code (which replaces the "minimum security measures" prescribed in the now repealed Presidential Decree No. 318/1999, issued to implement Section 15 of Law 675/96). These measures aim to ensure a

minimum level of personal data protection.

The "appropriate" precautions are governed by Section 31 of Legislative Decree No. 196/2003. When correctly adopted, they free the data controller from any form of liability (civil and criminal).

There are two types of minimum security measure depending on whether the personal data is processed "with" or "without" electronic means.

In the first case, Section 34 of the consolidated Data Protection Code lists eight different minimum measures:

- computer-based authentication;
- authentication credential management procedures;
- regular updating of the scope of the processing operations performed by individual data processors;
- protection of electronic means and data against unlawful or unauthorised access;
- procedures to generate backup copies and to restore data and system availability;
- maintenance of an up-to-date data security policy document;
- encryption techniques for processing operations performed by healthcare bodies.

Additional security measures are prescribed by individual general authorisations and in the guidelines regulating data processing for clinical purposes.

The obligation to adopt the minimum security measures prescribed in Section 35 of Legislative Decree No. 196/2003, especially those set forth from point 27 to point 29 of Schedule B, to which the reader is referred, also apply in the second case, i.e. when data is processed without the use of electronic means, which includes both traditional and hard copy formats.

The "appropriate" precautions are covered by Section 31 of the consolidated Data Protection Code. This Section requires data controllers processing personal data to introduce all suitable security measures needed to minimise "the risk of data being destroyed or lost, also by accident, the risk of unauthorised access to it, of unlawful processing operations or of processing inconsistent with the purposes for which the data was collected".

For this reason, if aligning a system with the minimum security measures releases a data controller from any criminal liability, it does not exempt the data controller from civil liability if, as a result of technological evolution, additional measures meeting the criteria of "appropriate" precautions become available.

This is because, according to Section 15 of the consolidated Data Protection Code, "Anyone who causes damage to another person as a consequence of the processing of personal data shall be liable to pay damages pursuant to Section 2050 of the Italian Civil Code". This means that the author of the data processing bears the objective responsibility for carrying out dangerous activities.

Section 2050 of the Civil Code prescribes that a body exercising a dangerous activity, the data controller in the present case, shall not be held liable provided that he/she can prove that all suitable precautions were taken to prevent any damage.

Otherwise, the data controller will also be liable for non-pecuniary damages, in accordance with Section 15, Subsection 2 of the consolidated Data Protection Code.

To meet the provisions of Section 2050 of the Italian Civil Code is not an easy task. According to court rulings, one can prove one has taken all suitable precautions if one can demonstrate compliance with "all known methods", even if only theoretically possible at the time [10].

From another point of view, it should also be underlined that in terms of the damages payable, the data controller would be liable for pecuniary damages (consequential loss or damage, and damage due to loss of income) and for moral damages, as can be concluded from the unequivocal wording of Section 15 of Legislative Decree No. 196/2003.

The explicit extension of non-pecuniary damages to the processing of personal data testifies to the lawmakers' desire to protect damaged parties, given that the most common damage normally sustained is to an individual's moral sphere, which would otherwise not be eligible for damages (based on Section 2059 of the Italian Civil Code).

In addition to the "minimum" measures, the data controller and the data officer must therefore also take "appropriate" precautions to reduce as far as possible any risks, both preventable and predictable ones, to the data collected.

PENALTIES

Civil and criminal liability for breach of Personal

Data Protection Code rules

All individuals bound to comply with the obligations of the Personal Data Protection Code but failing to do so will be held civilly and criminally liable, whether they are data controllers, data officers or data processors: in other words, all those involved in personal data processing operations but not adopting the conduct required of them by law.

First and foremost, it is important to distinguish civil liability from criminal liability.

A criminal offence is an act or omission punishable under criminal law. The penalties for criminal offences include life imprisonment, jail sentence, arrest or fine.

In contrast, an illegal act or breach of a regulation involves civil liability and the obligation to pay compensation for the damage caused.

In short, breaching a legal provision can result in criminal or civil liability, depending on the consequence envisaged by the law.

It will be criminal liability if the law assigns a penalty to the person committing the crime, and civil liability if the law envisages payment of damages. However, a wrongful act can invoke both criminal and civil liability.

The Personal Data Protection Code describes three types of liability, and therefore three different types of punishment.

Failure to abide by the provisions of the Personal Data Protection Code may involve civil liability, criminal liability or be considered as an administrative offence.

Civil offences are governed by Section 15 of the Personal Data Protection Code, which equates personal data processing with the dangerous activities defined in Section 2050 of the Italian Civil Code ("Anyone who causes damage to others while carrying out an activity that is dangerous either because of its nature or because of the means used to carry it out, shall pay compensation for the damages caused, unless it can be proved that he/she took all suitable precautions to avoid the damage").

The law refers to objective responsibility, such as liability for harm resulting from lawful acts, without specifying whether the harm resulted from an intentional or an accidental conduct.

The burden of proof is reversed under objective liability.

In the Italian civil courts, a plaintiff trying to exercise a right is faced with the difficult task of proving that the other party is liable and of demonstrating the extent of the damage underlying the claim; if they fail in this task, their claim will be rejected.

In the case of dangerous activities and pursuant to Section 15 of Legislative Decree No.196/2003, the burden of proof is reversed since they are construed as aggravated civil liability. The burden of proof therefore lies with the defendant to prove that, in using the data, all precautions were taken and all suitable technological measures introduced to avoid, or rather prevent, any damage. Clearly, it is insufficient to prove that a breach of law or common prudence was not committed; in this case positive proof is required to show that all appropriate measures to prevent any damage were taken.

There are four types of administrative offence and four different types of punishment: provision of inadequate or omitted information to the data subject (Section 161); other types of non-compliance (Section 162); incomplete or omitted notification (Section 163); failure to provide information or documentation to the Privacy Authority (Section 164) (Table 1).

In all of the above cases, the competent body invested with the authority to impose penalties is the Privacy Authority and the procedure is governed by Section 166 of Legislative Decree No. 196/2003.

The penalties are laid down in Title III of Part III of the Personal Data Protection Code.

The Code also lists the following types of criminal offence: unlawful data processing (Section 167), untrue declarations and notifications submitted to the Privacy Authority (Art. 168), security measures (Section 169), failure to comply with provisions laid down by the Privacy Authority (Section 170) (Table 2).

Data protection law in Italy requires close monitoring due to frequent changes that affect the regulatory framework and legal interpretation of provisions.

The most recent developments in the penalty system are contained in Law Decree No. 207 of 30 December 2008, converted by amendment to Law No. 14 of 27 February 2009.

The Personal Data Protection Code prescribes important obligations and numerous penalties, both administrative and criminal.

More specifically:

- security measures must be adopted, otherwise administrative penalties (payment

TABLE 1

ADMINISTRATIVE OFFENCES		
SECTION	DESCRIPTION	ADMINISTRATIVE OFFENCE
161 (1) As amended by Section 44, Subsection 2, of Law Decree No. 207 of 30 December 2008, converted by amendment to Law No. 14 of 27 February 2009.	Inadequate or omitted information to the data subject	(1) Breach of these provisions is punishable by an administrative fine of between 6 000 to 36 000 Euros (previously 3 000 and 18 000 Euros)
162 (1) As amended by Section 44, Subsection 3, letter a, of Law Decree No. 207 of 30 December 2008, converted by amendment to Law No. 14 of 27 February 2009 (2) As amended by Section 44, Subsection 2, letter b, of Law Decree No. 207 of 30 December 2008, converted by amendment to Law No. 14 of 27 February 2009 (3) Section added from Section 44, Subsection 3, letter c, of Law Decree No. 207 of 30 December 2008, by amendment of Law No. 14 of 27 February 2009, subsequently amended by Section 20b, Subsection 1, letter c, point 1, of Law Decree No. 135 of 25 September 2009, converted by amendment to Law No. 166 of 20 November 2009 (4) Subsection added from Section 44, Subsection 3, letter c, of Law Decree No. 207 of 30 December 2008, converted by amendment to Law No. 14 of 27 February 2009 (5) Subsection added from Section 20b, Subsection 1, letter c, of Law Decree No. 135 of 25 September 2009 converted by amendment to Law No. 166 of 27 November 2009	Other types of non-compliance	1.(1) Data transfer in breach of Section 16, Subsection 1, letter b, or of any other provisions regarding the processing of personal data is punishable by an administrative fine of between 10 000 and 60 000 Euros (previously 5 000 to 30 000 Euros) 2.(2) Breach of the provisions of Section 84, Subsection 1, is punishable by an administrative fine of between 1 000 and 6 000 Euros 2-b.(3) When personal data is processed in breach of the provisions set forth in Section 33 or of those laid down in Section 167, an administrative fine of between 10 000 and 120 000 Euros is also payable in any case. Reduced payments are not foreseen for the cases laid down in Section 33 2-c.(4) Failure to comply with the measures and prohibitions set out in Section 154, Subsection 1, letters c and d, is subject to an administrative fine of between 30 000 to 180 000 Euros 2-d.(5) Breach of the right to oppose the processing of one's personal data, as permitted under Section 130, Subsection 3b, and relevant regulation is punishable in accordance with Subsection 2b of the present Section
163 (1) As amended by Section 44, Subsection 5 of Law Decree No. 207 of 30 December 2008, converted by amendment to Law No. 14 of 27 February 2009	Incomplete or omitted notification	Anyone legally required to submit notification and not doing so in the term specified in Sections 37 and 38, or submitting incomplete information, is subject to an administrative fine of between 20 000 and 120 000 Euros (previously 10 000 to 60 000 Euros), and the accessory administrative penalty involving publication of the full version or abstract of the injunction in one or more newspapers specified in said injunction
164 (1) As amended by Section 44, Subsection 6, of Law Decree No. 207 of 30 December 2008, converted by amendment to Law No. 14 of 27 February 2009	Failure to provide information or documentation to the Privacy Authority	Anyone failing to provide the information or submit the documentation requested by the Privacy Authority in accordance with Section 15, Subsection 2, and Section157 is punishable with an administrative penalty fine of between 10 000 and 60 000 Euros (previously 4 000 to 24 000 Euros)

of a € 20 000-€ 120 000 fine) or criminal punishment (up to 2-year imprisonment) will be imposed;

- individuals processing sensitive data using electronic means must have a data protection policy document, and make sure it is updated by 31 March every year;

TABLE 2

CRIMINAL OFFENCES		
SECTION	DESCRIPTION	CRIMINAL OFFENCES
167	Unlawful data processing	Breach incurs a penalty, depending on the case, equal to a 6-18 months, 6-24 months or 1-3 years jail sentence, provided the action aimed to obtain a profit for oneself or for others, or to cause damage to others.
168	Submission of false information and notifications to the Privacy Authority	The applicable penalty is a 6 months-3 years jail sentence, provided that offence does not constitute a more serious crime
169 (1) As amended by Section 44, Subsection 9, letter a, of Law Decree No. 207 of 30 December 2008, converted by amendment to Law No. 14 of 27 February 2009 (2) As amended by Section 44, Subsection 9, letter b, of Law Decree No. 207 of 30 December 2008, converted by amendment to Law No. 14 of 27 February 2009	Security measures	1.(1) Anyone legally required to adopt the minimum security measures laid down in Section 33 but not doing so is punishable with 2-year imprisonment (or a fine of between 10 000 and 50 000 Euros). 2.(2) Upon verification or (in the more complex cases) in a subsequent provision from the Privacy Authority, the offender shall be given a legal prescription; the term set for compliance with the prescription shall be no longer than the time technically required to comply with it. This term can be extended for up to a maximum of 6 months in particularly complex cases where there is an objective difficulty meeting the term. If within 60 days of deadline expiration the prescription has been met, the Privacy Authority shall admit the offender to pay a fine equal to one fourth of the maximum penalty payable for an administrative offence. Meeting the prescription and paying the fine cancel the crime. The body issuing the prescription and the public prosecutor shall act as laid down in Sections 21, 22, 23 and 24 of Legislative Decree No. 758 of 19 December 1994, as amended
170	Failure to comply with Privacy Authority provisions	In the more serious offences, failure to comply with Privacy Authority provisions is punishable with a 3-month to 2-year jail sentence

- the Code enshrines the principle that personal data must be processed in full respect of the rights, dignity and confidentiality of the data subject;
- the scope of application within which data controllers and processors operate in their data processing must be clearly defined to promote a sense of responsibility;
- the Code requires damages to be paid when data processing causes damage to a data subject;
- the Code prescribes administrative fines from 6 000 to a maximum of 36 000 Euros in the event of inadequate or omitted information to the data subject.

CONCLUSIONS

This paper has been conceived as a tool to help researchers intending to use (and eventually to integrate) EMR data for epidemiological purposes find their way around Italian data protection law. Particular emphasis has been

placed on the confidential aspects of data and the anonymity of patients in scientific research; this issue is of great interest to the Privacy Authority [11]. We have explored other aspects, such as those connected with the nature of sensitive data, data ownership, and applicable penalties in the event of a breach of the relevant legal provisions.

SISMEC "OBSERVATIONAL STUDIES" WORKING GROUP MEMBERS. **Coordinators**. Gesuita Rosaria (Polytechnic University of Marche, Italy) Villani Simona (University of Pavia, Italy), Zambon Antonella (University of Milano-Bicocca, Italy). **Members**. Montomoli Cristina, Morandi Anna, Stendardo Antonietta (University of Pavia, Italy and Legal Study Nesci-Stendardo, Messina, Italy); Accordini Simone (University of Verona, Italy); Bamfi Francesco, Patarnello Francesca, Pitrelli Andrea (GlaxoSmithKline Italia, Verona, Italy); Biasi Valeria (University Hospital of Verona, Italy); Baldi Ileana, Gregori Dario, Frigo Annachiara (University of Padova, Italy), Volpato Sandra (Self-employed, Padova, Italy); Campari Cinzia, Vicentini Massimo (Local Health Unit of Reggio Emilia, Italy); Preite Francesca, (Legal Study Miari-Preite, Reggio Emilia, Italy - Medidata S.r.l., Modena, Italy); Simoni Lucia (Medidata S.r.l., Modena, Italy); Molinaro Sabrina (National Research Council, Pisa, taly); Galassi Gianmichele (University of Siena, Italy); Flavia Carle, Ferrante Luigi (Polytechnic University of Marche, Italy); Vestri Annarita (University of Roma "La Sapienza", Italy); Chiodini Paolo (Second University of Napoli, Italy); Trerotoli Paolo (University of Bari, Italy); Guardabasso Vincenzo (University Hospital of Catania, Italy); Minerba Luigi (University of Cagliari, Italy); Palmas Maria Antonietta (Healthcare Department of Region Sardinia, Italy); Solinas Giuliana, Sotgiu Giovanni (University of Sassari, Italy).

References

[1] Warren S and Brandeis L. The Right to Privacy. Harvard Law Review 1890; Vol IV, No. 5
[2] Rodotà S. Intervista su Privacy e Libertà. Paolo Conti Ed. 2005 Laterza, Bari-Roma
[3] Directive of the European Parliament and Council of 24 October 1995, 95/46/EC. The Official Journal of the European Union (OJEU-L), No. 281 23 November 1995: p. 31
[4] Official Journal of the Republic of Italy, No. 174 of 29 July 2003 - Ordinary Supplement No. 123
[5] Decision of the Privacy Authority of 13 October 1999, Bollettino Cittadini e Società dell'Informazione no. 11-12, p. 61)
[6] District Court for the Eastern District of Missouri 31 March 2006
[7] Wipo Treaty, Geneva 1996
[8] Auth. 24 June 2011 in the Official Journal of the Italian Republic, No. 159, 11 July 2011
[9] Auth. 24 June 2011 in the Official Journal of the Italian Republic, No. 162, 14 July 2011
[10] Milan Court ruling, 19 November 1987, Foro Italiano 1988; I: 144
[11] General authorisation to process personal data for scientific research purposes. Official Journal of the Republic of Italy, No. 72, 26 March 2012

*