B.I.R.O.

Best Information through Regional Outcomes

A Public Health Project funded by the European Commission, DG-SANCO 2005

WP 5

PRIVACY IMPACT ASSESSMENT (PIA)

REPORT 1

PRELIMINARY PRIVACY IMPACT ASSESSMENT

December 2006

The PIA Team

Privacy Facilitator:

- Dr. Concetta Tania Di Iorio, Legal Consultant, SeRectrix snc & C. Spoltore, ITALY

PIA Team Members:

- Dr. Marco Orsini, Dipartimento di Medicina Interna, Università di Perugia (UNIPG), ITALY
- Dr. Scott Cunningham, Division of Medicine & Therapeutics, University of Dundee (UNIDUND), SCOTLAND
- MSc Peter Beck, Institute of Medical Technologies and Health Management, Joanneum Research (JOANNEUM), Graz, AUSTRIA
- Dr. Sven Skeie, Department of Medicine, Section of Endocrinology, University of Bergen (UNIBERG), NORWAY
- Dr. Simion Pruna. Institute of Diabetes, Nutrition and Metabolic Diseases “N. Paulescu” (PAULESCU), Bucharest, ROMANIA
- Prof. Joseph Azzopardi, Department of Medicine, Universitat ta Malta (UNIMALT), La Valletta, MALTA
- Dr. Vivie Traynor, Department of Health Promotion, Ministry of Health (CYPRUS), Lefkosia, CYPRUS

The B.I.R.O. Consortium

The project is coordinated by :

- Prof. Massimo Massi Benedetti, Dipartimento di Medicina Interna, Università di Perugia (UNIPG), ITALY

The associated partners are:

- Prof. A. Morris, Division of Medicine & Therapeutics, University of Dundee (UNIDUND), SCOTLAND
- Prof. Thomas Pieber, Institute of Medical Technologies and Health Management, Joanneum Research (JOANNEUM), Graz, AUSTRIA
- Dr. Sven Skeie, Department of Medicine, Section of Endocrinology, University of Bergen (UNIBERG), NORWAY
- Dr. Simion Pruna. Institute of Diabetes, Nutrition and Metabolic Diseases “N. Paulescu” (PAULESCU), Bucharest, ROMANIA
- Prof. Joseph Azzopardi, Department of Medicine, Universitat ta Malta (UNIMALT), La Valletta, MALTA
- Dr. Rita Komodiki, Department of Health Promotion, Ministry of Health (CYPRUS), Lefkosia, CYPRUS

Table of Contents

Executive summary

BIRO is a three years public health program, carried out by the BIRO consortium, that aims at providing European health systems with an "ad hoc", evidence and population-based information system for diabetes, to support prevention, coordinated care and outcomes management on a continuous basis. The project targets a better integration of regional data collections, providing a new platform for the routine publication of summary indicators and the rapid updating of epidemiological models. The rationale of the project is that best information for health reports can be routinely collected through an alliance between regional initiatives that are already involved in the process. The BIRO Information System involves the use of sensitive-medical data collected through diabetes registries at national level and further processed for public health surveillance at international level.

In the first part of the project, the BIRO data flow involves a prospective number of patients in excess of 115,000. Technical planning requires formatting data for further manipulation. Each partner will prepare a "BIRO data export" that will allow the mapping of centres' data towards a common dataset, to be stored as an XML output. These files will be then loaded into a Postgres DBMS (WP6) that will manipulate data either directly, or via the statistical engine (WP8). This procedure will produce statistical objects that will be sent to the server via the communication software (WP9). The server hosts the central engine (WP10), which will be in charge of producing outputs in XML.

Details of the BIRO architecture still need to be defined. Nevertheless, BIRO partners have identified three possible alternatives underpinning the construction of the BIRO Information System.

The first solution is based on individual patients data, de-identified through the use of a pseudonym. In this case secure identity encryption algorithms have to be specified and privacy protective technology for securing the data transfer are to be implemented.

The second solution envisages the aggregation of patients' characteristics by groups of individuals, with Centre IDs still available, but subject to de-identification. The use of aggregated data requires the specification of secure encryption algorithms for Centre's identity and privacy protective technology for securing the data transfer.

The last option foresees an aggregation by region. In this case, there will be a need to specify optimised data aggregation that would still allow statistical analysis, though impeding reverse engineering. Privacy protective technology should be used for securing the data transfer as well.

Considering the characteristics of the diabetes registries involved in the project, processing operations that take place locally are subject to the exemption established in art. 8 (par. 3) of the Data Protection Directive. Each centre, independently from the BIRO project, collects information related to an identified or identifiable natural person for the purpose of setting up a disease registry. Hence, it can be inferred that those data are collected and processed for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment, or the management of health care services. According to the EU Data Protection Directive, consent from the data subject may not be required in those cases, unless domestic laws provide more stringent regulations.

From the same regulation follows that, should the BIRO centres provide for the de-identification of data before transferring them to the central database (where data will be processed for statistical and scientific purposes), this processing operation would be legally compatible with the purposes

for which data have previously been collected. As a general rule, the further processing of personal data for statistical or scientific research purposes is in fact considered, within the EU Directive, compatible with the purposes for which the data have previously being collected.

Furthermore, the Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) considers the use of data for statistical work as examples of no-risk data processing operations, in so far as those data are presented in aggregate form and stripped of their identifiers. Similarly, scientific research is included in this category.

As far as transborder data flow is concerned, three international instruments are essentially relevant: art 12 of the Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data (1981), art. 11 of the Council of Europe Recommendation on Medical Data and art. 25 of the EU Data Protection Directive (1995).

In synthesis, these regulations state that Contracting States (of the Convention) or Member States (of the EU) cannot pose obstacles to transborder data flows, even when medical data are involved, in the form of prohibitions or special authorisations of data transfers. Such States, having subscribed to a common core of data protection provisions, offer an adequate level of privacy protection.

The Centres involved in the BIRO project belong to European countries that have fully implemented the EU Data Protection Directive and ratified the Convention; hence, an adequate level of privacy protection is fully guaranteed across the countries involved. This means that the exchange of data envisaged in the project is not only legally viable, but also favoured by EU and international legislation. As anticipated, the BIRO Information System will process only de-identified data. Hence, the level of risk posed to privacy is to be considered very low. Nevertheless, it is crucial to foresee any possible breach of privacy through the adoption of appropriate technologies ensuring that encryption algorithms will be efficient and produce a secure environment for the data processed. For instance, it is fundamental to guarantee that reverse engineering will be impeded through appropriate mechanisms. Since the BIRO project will develop a database, SEDIS, to be hosted by the University of Perugia, Italy, the Italian legislation about security requirements will be also adhered to. The set of techniques identified by the Italian legislation are attached to the Italian Data Protection Code[1], constituting its Annex B.

The present report concentrates on the Preliminary Privacy Impact Assessment of the BIRO project. It includes a summary description of the project, the legislative framework, the data flow and information system's architecture and of possible privacy risks related to the implementation and management of the BIRO Information System, along with a description of possible mitigation strategies. The implementation of privacy enhancing technologies and security solutions is also envisaged.

The privacy impact assessment of the BIRO project will proceed through four steps: step 1: Preliminary PIA, step 2: Data flows Analysis, Step 3: Privacy analysis and Step 4: PIA Report.

[1] Decreto legislativo 30 giugno 2003, n. 196, CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI, aggiornato alla legge 12 luglio 2006, n. 228 di conversione, con modificazioni, del decreto-legge 12 maggio 2006, n. 173. Available at:

http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Normativa%2FItaliana%2FIl+Codice+in+materia+di+protezione+dei+dati+personal

1. Introduction

1.1 Rationale for the Preliminary PIA

The choice of conducting a Preliminary Privacy Impact Assessment (PIA), instead of proceeding directly to the first step of a full PIA (project initiation/need assessment), resides in the fact that the BIRO project is yet at an early design stage and lacks sufficient information to conduct a full PIA. In particular, the available information would not allow the identification of all the types and volumes of personal information that are to be collected, used and disclosed. Consequently, it would be difficult to identify with precision the legislative and policy framework of the BIRO Information System and, therefore, to determine which aspects of the project are likely to involve privacy risks.

1.2 The PIA Team

The PIA Team is composed of a representative for each partner of the BIRO Consortium, and ensures the following expertise:

- Privacy and legal expertise: to provide advice and recommendations with respect to relevant legislation, regulations, rules, privacy issues, current privacy developments, national and international privacy standards, possible conflicts etc.
- Technology and systems expertise: to provide technical and systems advice on mainframe and legacy systems, Internet tools and system interfaces, information, security, technical architecture and data flows
- Information and records keeping skills: to provide advice on how records are to be kept and information retained.

The Team will remain active for the entire duration of the project.

1.3 Report Objectives & Scope

The Preliminary PIA report aims at providing a summary description of possible privacy risks in the implementation and management of the BIRO Information System. A summary privacy legislative framework will be identified and regularly updated during the implementation of the full PIA, as design changes occur. The full PIA Report will provide a definitive description of privacy risks, applicable privacy legislation and mitigation strategies.

The present report identifies three main alternatives for the development of the BIRO architecture, based on the original proposal and selected after reviewing the relevant literature in the field of privacy of information systems, databases and registries in the health sector. Security issues and privacy enhancing technologies have also been examined.

The report provides a summary evaluation of privacy risks associated to the BIRO architecture, along with a description of possible mitigation strategies. The implementation of privacy enhancing technologies and security solutions is also considered.

The report allows refining the BIRO architecture according to privacy requirements/criteria and will be used as source of information in the full PIA.

In consideration of the evolutionary framework of the BIRO Information System, a continuous updating process is required to reflect any system change. The results of the BIRO Preliminary PIA will provide the fundamental information requested for the safe and durable development of the full assessment.

Ultimately, the Preliminary PIA, which underpins the realization of the full PIA, provides a balanced approach to realize the best, most privacy protective solution for the BIRO Information, identifying the very best possible solution.

2. Project background/ Description

2.1 Abstract

The present project, carried out by the BIRO consortium, aims to provide European health systems with an ad hoc, evidence and population-based information system for diabetes, to support prevention, coordinated care and outcomes management on a continuous basis.

The project targets a better integration of regional data collections, providing a new platform for the routine publication of summary indicators and the rapid updating of epidemiological models.

BIRO is a three years program that will link the existing knowledge base to regional datasets through specialised software. The rationale of the project is that best information for health reports can be routinely collected through an alliance between regional initiatives that are already involved in the process.

The proposed application is based on robust data and a high quality network of partners managing established and widely referenced diabetes registers across Europe, including Scotland, Norway, Austria and Italy.

The BIRO project, by assembling results from massive data sets through autonomous mechanisms, will allow analysing and modelling public health actions for diabetes at the regional, national, and European level.

A system of novel tools is being implemented for the purpose of populating schemes produced by recent European projects in the field of diabetes. A qualified team of partners from acceding and candidate countries (Malta, Cyprus, Romania) are fully involved in the project for the construction of a shared network that could be easily expanded and become widely used across Europe.

The production of open software will allow transferring this approach to other regions and other diseases, contributing to build an intelligent environment for population health reporting.

2.2 General objectives

The project aims to build a knowledge base that can be continuously updated for the general purpose of:

a) Enhancing the EU capacity to combat a specific health concern, diabetes, that is progressively affecting the portion of the population at highest risk, e.g. those presenting multiple risk factors and diseases, subjects obese, impaired, socially excluded, aged;

b) Supporting EU policy-making through a systems approach for the evaluation of different strategies for health care and prevention.

The proposal offers an efficient and sustainable solution for the following tasks:

- analysis of longitudinal trends and average outcomes in a diabetic population
- identification of patterns of care and prevention consistently showing positive results
- identification of population strata and/or practices that do not show effective results
- verification of the application/applicability of best practice guidelines
- on-field testing of collaborative information systems in chronic diseases

2.3 Specific objectives

Specific objectives of the project are the following:

a) to embed available clinical guidelines in a shared information system

b) to connect databases from different regions using minimum datasets specifically created for international comparisons

c) to build algorithms for the automatic construction and update of all diabetes-related health indicators

d) to bring all definitions together in a concept and data dictionary

e) to define a range of target analyses to be conducted through report templates.

f) to design and implement the relational data model and the statistical methods required for reporting

g) to validate a secure protocol for international communication and shared data analysis

h) to develop all software using approaches that will ensure wide usability in the public domain

i) to link the different components together in a user-friendly reporting facility

j) to start automatic production of health reports on a web portal and disseminate results of the project.

2.4 Statistical methods

Modern database techniques and advanced statistical methods will be used to collect and analyse population-based data stored in diabetes registries.

Statistical models will include generalized/longitudinal linear models, survival, GEEs and multilevel models, the latter to take into account different sources of variation.

Meta-analyses will be used to exploit data transfer across countries using aggregate tables. Risks of this project relate to the difficulty of using different sources of information.

We plan to reach consensus and a high level of standardization through strong collaborative links and processes that will involve participants at all stages.

The method of systematic review will be used whenever possible to drive evidence-base choices on the construction of a common information system (concept/data dictionary).

Possible difficulties in the interoperability of different software will be avoided through the development of multi-platform tools and open source solution.

3. Legislative Framework

3.1 Introduction

Major developments have occurred in traditional research fields during the last century, and new fields are continually expanding new and old disciplines.

Phenomena such as the growth of health informatics, the capabilities of on-line health information systems, the increasing importance of "evidence based medicine", and the impact of resource constraints on the health sector have all produced rapid changes in health information systems all over the world, provoking an increasing demand for accessing health information for research purposes.

As a result, the availability of patient's longitudinal health information is nowadays fundamental for improving public health.

Although research claims to patient data are justified by potential benefit for the health of the public, the importance and the benefits of research have to be weighted against the burdens undertaken by those participating in research; and privacy protection is a crucial component for balancing these conflicting interests.

3.2 The Right to Privacy

Of all the human rights in the international catalogue, privacy is perhaps the most difficult to define[2].

Definitions of privacy vary widely according to contexts and environments. Nevertheless, privacy is usually seen as the way of drawing the line of how far society can intrude into a person's private life.

Privacy has been defined as the "right to be left alone"[3]; or as "the right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information[4].

Although there is a lack of a single definition of privacy, it has been argued that "in one sense, all human rights are aspects of the right to privacy"[5].

Indeed, privacy is a human right generally recognized around the world and crystallised in many international instruments.

The 1948 **Universal Declaration of Human Rights** was the first international binding instrument

---

[2] James Michael, Privacy and Human Rights 1. (UNESCO) 1994. Available at: http://webjcli.ncl.ac.uk/articles1/davies1.html

[3] Samuel Warren, Louis Brandeis. The Right to Privacy. Harvard Law Review 1890; 4:193–220

[4] (Chairman) David Calcutt QC. Report of the Committee on Privacy and Related Matters. London: Cmnd. 11027, 1990

[5] Volio Fernando. Legal Personality, Privacy and the Family. Henkin ed. The International Bill of Rights: Columbia University Press, 1988

to recognise privacy as a human right, specifically protecting territorial and communication's privacy[6]. Article 12 states: *"No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks".*

In addition, numerous international human rights treaties specifically recognize privacy as a right. The International Covenant on Civil and Political Rights (ICCPR – art. 17)[7]; the UN Convention on Migrant Workers (Article 14)[8], and the UN Convention on Protection of the Child (Article 16)[9] adopt the same language. On the regional level, various treaties make these rights legally enforceable.

For instance, Article 8 of the **European Convention for the Protection of Human Rights and Fundamental Freedoms** (1950)[10] states that *"Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health of morals, or for the protection of the rights and freedoms of others".*

The Convention created the European Commission of Human Rights and the European Court of Human Rights to oversee enforcement. Both have been active in the enforcement of privacy rights, and have consistently viewed Article 8's protections expansively and interpreted the restrictions narrowly[11].

---

6 Universal Declaration of Human Rights, adopted and proclaimed by General Assembly resolution 217 A (III) of December 10, 1948 Available at <http://www.un.org/Overview/rights.html>.

7 International Covenant on Civil and Political Rights, adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of December 16, 1966, entry into force March 23rd 1976. Available at <http://www.unhchr.ch/html/menu3/b/a_ccpr.htm>.

8 International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, adopted by General Assembly resolution 45/158 of December 18, 1990, available at <http://www.unhchr.ch/html/menu3/b/m_mwctoc.htm>.

9 Convention on the Rights of the Child, adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of November 20, 1989, entry into force September 2, 1990. Available at: <http://www.unhchr.ch/html/menu3/b/k2crc.htm>.

10 Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, (ETS no: 005) open for signature November 4, 1950, entry into force September 3, 1950. Available at: <http://conventions.coe.int/Treaty/EN/cadreprincipal.htm>

11 Strossen Nadine, Recent United States and Intl. Judicial Protection of Individual Rights: A comparative Legal Process Analysis and Proposed Synthesis. Hastings Law Journal 1990; 41: 805

The Court has reviewed member states' laws and imposed sanctions on numerous countries[12]; and has also reviewed cases of individuals' access to their personal information in government files to ensure that adequate procedures exist[13]. In the evolution of data protection, the interest in the right of privacy increased in the 1960s and 1970s with the advent of information technology.

The surveillance potential of powerful computer systems has increased the demand for specific rules governing the collection and handling of personal information.

Two crucial international instruments in the evolution of data protection are the Council of Europe's (1981) Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data[14], and the Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data[15], which set out specific rules covering the handling of electronic data.

These rules describe personal information as data that have accorded protection at every step: from collection to storage and dissemination.

As a matter of fact, the above-mentioned agreements have had a profound effect on the enactment of laws around the world.

Nearly thirty countries have signed the COE Convention; and the OECD guidelines have been widely used in national legislations, even outside the OECD member countries.

The development of privacy protection in the EU took a step forward with the Council of Europe Convention on Human rights and Biomedicine (Oviedo 1997), which reinforced the principles that everyone is entitled to the right to privacy and confidentiality of personal medical data and the right to be informed about his/her health[16].

Finally, the **Charter of Fundamental rights of the European Union** (2000/C 364/01)[17] specifically provides protection of personal data.

---

[12] European Court of Human Rights, Case of Klass and Others: Judgement of 6 September 1978, Series A No. 28 (1979). Malone v. Commissioner of Police, Series A82 (1984). Available at: http://hudoc.echr.coe.int/hudoc/ViewRoot.asp?Item=5&Action=Html&X=1007095902&Notice=0&Noticemode=&RelatedMode=0;

[13] European Court of Human Rights, Leander v. Sweden, series A No 116 (1987). Available at: http://hudoc.echr.coe.int/hudoc/ViewRoot.asp?Item=0&Action=Html&X=1007101431&Notice=0&Noticemode=&RelatedMode=0

[14] Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data Convention. Strasbourg, 1981. Available at: http://www.coe.fr/eng/legaltxt/108e.htm

[15] OECD, Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data. Paris, 1981. Available at: http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM

[16] Council of Europe Convention on Human rights and Biomedicine (Oviedo 1997), Available at: http://conventions.coe.int/Treaty/EN/Treaties/Html/164.htm

[17] Charter of Fundamental Rights of the European Union (2000/C 364/01) Available at: http://ec.europa.eu/justice_home/unit/charte/index_en.html

Art 8 states: "*Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data, which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority".*

The Charter of Fundamental Rights has been fully incorporated in the **European Constitution** (forming its part II)[18], signed in Rome on the 29th of October 2004.

Although the Parliament, the Council and the Commission solemnly proclaimed the Charter on the 8th of December 2000, the Charter was not part of the Union's Treaties and therefore it had no binding legal force.

The Constitution thus achieved a major breakthrough, which allows the Union to have its own catalogue of rights, binding for all European countries and enforceable through the Court of Justice, which will in fact ensure that the Charter will be adhered to.

It is worth noting that the content of the Charter is broader than that of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), signed in Rome on 4 November 1950 and ratified by all the Member States of the Union.

Whereas the ECHR is limited to civil and political rights, the Charter of Fundamental Rights covers other areas such as the right to good administration, the social rights of workers, the protection of personal data and bioethics.

Finally, The **Additional Protocol to the Convention on Human Rights and Biomedicine, concerning Biomedical Research** (2005)[19] further reinforced the duty of confidentiality in the handling of personal information in health research and reaffirmed the obligation to treat them according to the rules relating to the protection of private life.

3.3 The EU Data Protection Directive (95/46/EC)[20]

The EU has adopted a privacy model that embraces comprehensive laws. The model is based on a general and abstract law that governs all aspects of the handling of personal information: from collection to use and dissemination, by both the public and private sectors.

The Directive in fact refers, in general, to the "**processing**" of personal data, including "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such us collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction".

Importantly, article 2 defines what is meant for "**personal data**", namely: any information relating

[18] Official Journal of the European Union C 310 Volume 47 of 16 December 2004. Available at: http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2004:310:SOM:EN:HTML

[19] Additional Protocol to the Convention on Human Rights and Biomedicine, concerning Biomedical Research. Strasbourg, 25.I.2005. Available at: http://conventions.coe.int/Treaty/EN/Treaties/Html/195.htm

[20] Directive 95/46/EC. Available at: http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

to an identified or identifiable natural person. Article 2 further explains the notion of identifiable person, which means any person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or societal identity.

The 1995 Data Protection Directive set up a common level of privacy among European countries, ensuring compliance through the establishment of a regulatory body.

The Directive not only reinforced current data protection laws, but also established a range of new rights and basic principles, namely: the right to know where the data originated, the right to have inaccurate data rectified, a right of recourse in the event of unlawful processing, and the right to withhold permission to use data in some circumstances. The Directive contains strengthened protections over the use of sensitive data.

Art 7 of the Directive establishes a set of criteria of "legitimate processing". Processing, in order to be legitimate, has to take place: either with the unambiguous consent of the data subject, or where this is necessary for the performance of a contract with the data subject, for compliance with a legal obligation, or for the performance of a government task, just to mention a few examples.

More stringent conditions apply to the processing of special categories of **sensitive data**, such as medical data. Here, the processing of sensitive data is considered, in principle, not legitimate and member states has to prohibit their processing, unless special conditions verify.

The art. 8 prohibition not apply when:

- the data subject has given his explicit consent to the processing of those data, or
- processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
- processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or
- processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or
- the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

Importantly, the prohibition of Article 8 (1) shall, according to Article 8 (3), also not apply where the data are required:

- for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and

- where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

Moreover, Member States may, according to Article 8 (4), for reasons of substantial public interest, lay down exemptions, in addition to those laid down, either by national law or by decision of the supervisory authority.

Art. 8(3) is extremely important for the health sector, since justifies the collection, use, and processing of health data, for the specified purposes, without the patient's consent.

Although the free and informed consent will be necessary if, for instance, those data would be further used for research purposes. The reference to professional secrecy contained in art. 8 (3) is crucial for obtaining a more effective protection of privacy in the handling of sensitive health data. Although the issues surrounding the confidentiality of health data are not fully dealt with in the Directive, the referral to the obligation of confidentiality in the Directive represents a step forward towards an eventual harmonization of European legislations.

At least, it imposes to Member States, in a binding form, the **duty of confidentiality** to any person involved in the processing of personal sensitive data. The duty of confidentiality was indeed traditionally linked to the duty of professional secrecy incumbent on health professionals (either through a law or code of conduct), but it did not directly involve any other subjects who might in fact handle health data. Privacy and confidentiality, even if often confused among them, are conceptually different and traditionally tackled separately.

The principle of confidentiality of medical information is derived by the Hippocratic Oath, and can be considered one of the oldest principles applying to data protection; on the contrary, privacy as a right is a concept developed in modern times. Nevertheless, the two principles are strictly interrelated and need to be consistently implemented among European countries in order to enhance the protection of privacy when sensitive data are involved.

Importantly, the 1995 Directive imposes an obligation on member states to ensure that the personal information relating to European citizens has the same level of protection when it is exported to, and processed in, countries outside the EU.

As a result, countries refusing to adopt adequate privacy laws may find themselves unable to conduct certain types of information flows with Europe, particularly if they involve sensitive data.

3.4 Council of Europe Recommendation No. R (97) 5 [21]

In 1997, the Council of Europe enacted a Recommendation on the Protection of Medical Data. The recommendation acknowledges that medical data require even more protection than other non-sensitive personal data, reaffirming that the respect of rights and fundamental freedoms, and in particular of the right to privacy has to be guaranteed during the collection and processing of medical data.

[21] Council of Europe Recommendation No R (97) 5; Available at: http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/international_legal_instruments/Rec(97)5_EN.pdf

For those reasons, Principle 3.2 recalls the requirement in Article 6 of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) for appropriate safeguards in the law, in so far as the various stages of collection and processing of medical data are concerned.

According to the Recommendation, **the processing of medical data is, in principle, prohibited, unless appropriate safeguards are provided by domestic law.**

One of such safeguards is that only health-care professionals, bound by **rules of confidentiality**, should collect and process medical data, or where necessary persons acting on behalf of health-care professionals, as long as such persons are subject to the same rules.

Since the definition of health professional may vary across different countries, the recommendation provides for the possibility that personnel not directly responsible for health care may collect and process medical data; but only on the condition that this category of professionals must abide by confidentiality rules comparable with those imposed on health-care professionals, or that domestic law provides for appropriate safeguards which are as efficient as confidentiality rules, that is, they are efficient enough to guarantee respect of privacy of the data subject.

Once again, with a view to the sensitive nature of medical data, Principle 4.1 recalls the provisions in Article 5 of the Convention: the collection and processing of medical data must be fair and lawful, and for specific purposes only.

The **principle of fair collection** is made more explicit in Principle 4.2: medical data must, in normal conditions, be obtained from the data subject himself/herself. This principle therefore concerns the "disclosure" of these data by the data subject himself/herself, and not "communication" of medical data by a third party (for example, the doctor).

Principle 4.3 lays down the rules governing the collection or processing of medical data. The latter may be collected or processed: if it is provided for by law, there is a contractual obligation to do so, if this is necessary for the establishment of a legal claim or if the data subject has given his/her consent. Principle 4.3 does not constitute derogation from Principle 3.2, but sets conditions for the legitimacy of the collection or processing.

Medical data may also be collected from the data subject or from other sources if this is provided for by the law for one of the purposes set out in Principle 4.3(a): for public health reasons, the prevention of a real danger or the suppression of a specific criminal offence, or another important public interest.

Furthermore, medical data may be collected and processed if permitted by law for the purposes set out in *Principle 4.3 (b): for preventive medical purposes or for diagnostic or therapeutic purposes (in this case data may also be processed for the management of medical service operating in the interest of the patient), or to safeguard the vital interests of a data subject, or with a view to respecting specific contractual obligations, or with a view to the establishment, exercise or defence of a legal claim.*

In accordance with principle 4.3 (c), medical data may also be collected and processed if the data subject has given his/her consent for one or more purposes in so far as domestic law does not provide otherwise.

Medical data may therefore be collected without consent, if the law provides for this, "for the purposes of" (that is, in the interest of) public health; this purpose is in line with the derogation for reasons of public safety in Article 9 of the Convention. It should also be noted that the words "in the interest of public health" include the management of health services.

One of the means to ensure that medical data are obtained and processed fairly and lawfully is to inform the data subject whose data are collected of a number of elements (**information to be given to the data subject**). These elements are listed in Principle 5.1. It is obvious that such provision of information is indispensable when the data subject is required to give his/her "informed" consent (see paragraph 130 hereafter). But even in cases where his/her consent is not required - that is, when the collection and processing of medical data follow an obligation under the law or under a contract, are provided for or authorised by law, or when the consent requirement is dispensed with - the recommendation provides that the data subject is entitled to relevant information. Although Principle 5.1 should be interpreted strictly, two kinds of derogation are admitted. First of all, Principle 5.6 allows for derogations to be made for certain reasons of public interest, for protection of the data subject or a third person, or in medical emergencies. Secondly, information on the various elements listed in the principle has to be supplied only in so far as it is relevant.

Principle 5.1 identifies the following elements on which the data subject must be informed:

- the existence of a file containing his/her medical data and the type of data collected or to be collected;
- the purpose or purposes for which they are or will be processed;
- where applicable, the individuals or bodies from whom they are or will be collected
- the persons or bodies to whom and the purposes for which they may be communicated
- the possibility, if any, for the data subject to refuse his consent, to withdraw it and the consequences of such withdrawal;
- the identity of the controller and of his/her representative, if any, as well as the conditions under which the rights of access and of rectification may be exercised.

One of the conditions on which medical data may be collected and processed is that the data subject has given his/her **consent,** in so far as he/she is capable of doing so. As these data are regarded as sensitive data, Principle 6.1 requires that the consent be "free, express and informed".

Consent is "informed" if the data subject is informed in particular of the purposes involved and the identity of the data controller. Consent is "free" if the data subject has the possibility to refuse his/her consent, to withdraw it or to modify the terms and conditions of consent. Consent can be expressed orally or in writings.

However, under certain conditions, medical data could be processed without the data subject's free, express and informed consent. These conditions are listed exhaustively in the recommendation.

As regards the collection of medical data in the course of a consultation or treatment for

preventive, diagnostic or therapeutic purposes by a doctor, and which the data subject has freely chosen, the consent of the patient may not need to be expressed if the data were indeed to be processed only for the provision of care to the patient. This is also valid for processing medical data in the context of the management of a medical service operating in his/her interest.

The recommendation reaffirm the **right of access**: every person has to be enabled to have access to his/her medical data, either directly or through a health-care professional. Importantly, art. 8 (1) of the recommendation states that the information must be provided to patients "in understandable form". Access to medical data may be refused, limited or delayed only if the law provides for this.

The data subject has also the right to rectification: patients may ask for rectification of erroneous data concerning him/her and, in case of refusal, he/she has to be able to appeal.

In general, medical data shall be kept no longer than necessary to achieve the purpose for which they were collected and processed (conservation).

Although the recommendation does not refer to it explicitly, the requirement in Article 5 of the Convention that personal data undergoing automatic processing should be adequate, relevant and not excessive applies equally to medical research. It means that only the data necessary for the purposes of such research should be used.

The primary means of protecting medical data to be used for **scientific research** purposes is to make them anonymous. For this reason, researchers as well as public authorities concerned are urged to develop anonymisation techniques.

The nature or objectives of certain research projects sometimes make it impossible to use anonymous data. In such cases, under Principle 12.2, personal data may be used if the purposes of the research project are legitimate and one of the listed conditions is fulfilled.

Firstly, personal data may be used for medical research if the data subject has been duly informed of the research project - or at least if the information requirements have been respected - and has given his/her consent for that particular project, or, at least, for the purposes of medical research

Secondly, in the case of a legally incapacitated person, this consent must have been given in accordance with Principle 6.4, and the research project must have a connection with the medical condition or disease of the data subject (sub-paragraph b). This is provided to avoid that consent given on behalf of a legally incapacitated person might be motivated by material interests.

Thirdly, cases may arise where the data subject cannot be found or where for other reasons it is apparently impossible to obtain consent from the data subject himself/herself (for example, in the case of an epidemic). When in such cases the interests of the research project are such that they justify the consent requirement to be waived - for example in the case of an important public interest - and unless the data subject has explicitly refused any disclosure, then the authorisation to use personal data may be given by the body or bodies designated by domestic law and competent in the area of personal data. Such authorisation should, however, not be given globally, but case-by-case; moreover, the medical data should be used only for the medical research project defined by that body, and not for another project of the same nature (sub-paragraph c).

The authorisation, by the designated body, of communication of medical data for the purposes of a medical research project also depends on other factors implicit in the spirit of the recommendation in the present principle, or explicitly set out in other principles:

- the existence of alternative methods for the research envisaged;
- the relevance of an important public interest of the aim of the research, for example in the field of epidemiology, of drug control or of the clinical evaluation of medicines;
- the security measures envisaged to protect privacy;
- the necessity of interfering in the privacy of the data subject.

Under sub-paragraph (c), it would not be necessary to make the reasonable efforts in all cases; the person in charge must, however, consider whether with reasonable efforts it would be practicable to contact all data subjects. If this seems possible, then the efforts must be made. Furthermore, it was understood that to seek the consent of the data subject for medical research would be an unreasonable demand for the research institute, and would rather be the responsibility of the person or body envisaging disclosure of medical data.

According to article 12 (3), subject to complementary provisions determined by domestic law, health-care professionals entitled to carry out their own medical research are allowed to use the medical data which they hold, as long as the data subject has been informed of this possibility and has not objected. In addition, art. 12(4) explore the possibility that scientific research based on personal data might raise incidental problems, including those of an ethical and scientific nature, relative to the respect of the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. In this case, the norm recommends examining them also in the light of other relevant instruments.

Finally, personal data used for scientific research must not be published in a form, which enables the data subjects to be identified, unless they have given their consent for the publication and domestic law permits publication.

3.5 The Need for Secondary Uses of Health Information

Information exchange has become a crucial element in all fields of research and technological development. Nowadays, international research programs are frequently based on computerised systems for remote access, concurrent data processing, and secure online transmission, which together form an infrastructure that is becoming essential for health research. Nonetheless, the evolution of science has to balance the spread of new technologies with ethical values, cultural differences, and legislations. The respect of privacy in the handling of personal data is widely acknowledged as a core feature of data processing technologies. As a matter of fact, privacy is a fundamental human right recognized internationally in many binding agreements, which have set out specific rules covering the handling of electronic data.

In all international agreements, health information is regarded as 'sensitive' data and consequently it is regulated with a greater level of protection within privacy legislations.

Undoubtedly, the processing of health data is central to health research, and the public interest in health research can hardly be questioned. Data linkage has been proved essential for health care evaluation, for the estimation of the effects of public health programs, for the containment of health expenditure, and for the implementation of cost-effective financing systems. As a result, researchers increasingly link clinical records, disease registers, vital statistics, systems for environmental surveillance, and databases from heterogeneous sources.

A fundamental assumption can be drawn from privacy legislations is that the purpose of medical records and health information is to assist the health care provider in managing the patient. Under this model, other uses of personal information have to be considered extraordinary, in the sense that they require special permission or some mechanisms that aim at balancing patients' interests with the competing interests that favour secondary uses. Health and biomedical research in EU countries is consistent with this model.

However, there has been an increasing interest, in recent decades, in the 'secondary use' of clinical information, which is the use of personal data for public health surveillance and research. This trend has received further impetus because of the developments in information technology and health informatics, which strongly relay on a strategic 'secondary use' of health data.

The current approach to public health is based on the assumption that economic, environmental, ecological, political and behavioural components strongly influence human health and that health problems are characterised by interdependence with one another, and by interdependence with life style and environment[22].

Indeed, the capacity to link data from clinical records, disease registers and other health databases, demographic data (for example, census data), environmental surveillance data, socio-economic data, patient-reported data (such as tobacco use) is vital to capture the significance of the lifestyle and environmental factors that impact on mortality and morbidity.

As a matter of fact, population-based health information systems are integrated with a variety of

[22] Kirby R. From Public Health to Population Health: Epidemiological Yardsticks for Perinatal Care. Journal of Perinatology 1988; 19: S. 16-18

external data sources to provide a comprehensive perspective on the determinants of health. Since both economic benefits and health gains are expected from public health studies, these trends towards a 'strategic use' of health data are likely to intensify the demand for the 'secondary use' of patient data in public health and clinical outcomes research.

In obtaining evidence of exposures and health outcomes, researchers in fact need to access data held in health registers and databases, as sources of information separate from clinical records.

In particular, medical registries have become increasingly important, for instance, for the care of patients and the evaluation of health outcomes after the implementation of disease prevention and treatment programs.

They have also become vital to quality-improvement programs that assess the safety of new drugs and procedures, identify best clinical practice and compare health care systems[23]. On the other hand, registries require the collection and processing of data in an identifiable form in order to allow, among the others, patient's follow-up. This kind of processing necessarily raises privacy and confidentiality issues. However, the quality and completeness of data included in registers is extremely important to avoid biases that would affect the generalization and applicability of results. Hence, although privacy must be safeguarded, privacy norms should be consistent with the goal of obtaining complete data[24]. In conclusion, the increasing secondary use of health information and the necessity to ensure data quality for the provision of better care, accrued the tension between health research and privacy. Although privacy principles and legislations may constrain health research, the right to privacy is not an absolute right. The right to privacy has in fact to be weighed against matters that benefit society as a whole, including health research.

In the light of both improving the health of the public and protecting patient's rights, it is extremely important to guarantee reasonable levels of privacy, without unnecessarily constraining scientific investigation.

3.6 Data protection principles

The expression of data protection in different laws and regulations varies.

However, data protection laws have all adopted a set of core principles in regulating the processing of personal data, which are drawn upon the EU and international instruments.

The core data protection principles are:

- Fairness and lawfulness of processing
- Minimality
- Purpose specification
- Information quality

---

[23] Owen D Williamson. Medical Registry Governance and Patient Privacy: MJA 2004; 181 (3)

[24] Julie Ingelfinger, Jeffrey Drazen. Registry Research and Medical Privacy. The New England Journal of Medicine. 2004; 350 (14)

- Data subject participation and control
- Disclosure limitation
- Information security and
- Sensitivity

It is worth considering that these categories frequently overlap and, at the same time, each category may express multiple principles. Consequently, some aspects of a principle may be contained in one or more principles.

The above principles are primarily abstractions of a set of legal rules. They are crucial because they have obtained normative force in most European countries, guide data protection authorities in the exercise of their discretionary powers and Ethics Committee in the evaluation of health research projects. They also conditioned the shaping and drafting of new data protection laws. This is evident by considering the influence the 1980 OECD Data Protection Guidelines (OECD Guidelines) have had on the drafting of the legislation of most OECD member states and even outside OECD countries.

The primary principle of data protection laws is that personal data should be 'processed fairly and lawfully[25]. This principle is 'primary' because it both embraces and generates the other core principles of data protection laws. While the notion of lawfulness is relatively self-explanatory, the one of fairness is very broad in meaning and it is almost impossible to give a univocal interpretation across different legislations.

At a very general level, it means that the collection and further processing of personal data must be carried out in a manner that does not intrude unreasonably upon the data subjects' privacy nor interfere unreasonably with their autonomy and integrity.

In other words, fairness requires balance and proportion both at the level of individual data processing operations and at the design stage of information systems supporting such operations.

The notion of fairness also implies that the data subject should not be pressured to give data concerning himself, which is a principle backed up by the informed consent norms, which impose that consent has to be freely given[26].

The notion of fairness also means that the data subject be informed of the processing and of the purpose of the processing. Another assumption that could be drawn by the principle of fairness is that data should, in principle, be collected directly from the data subject[27].

---

[25] At an international level, see for example art 5(a) of the 1981 Council of Europe Convention on Data Protection (CoE Convention) and art 6(1)(a) of the 1995 EC Directive on Data Protection (EC Directive). At a national level, see for example art 9 of Italy's 1996 Law on Protection of Individuals and Other Subjects with Regard to Processing of Personal Data and Data Protection Principle 1 in Sch 1 to the UK Data Protection Act 1998.

[26] See, for example, art 6(1) of the Council of Europe Recommendation on the Protection of Medical Data; No. R (97) 5.

[27] The link between fairness and transparency is made explicit in, inter alia, recital 38 of the EC Directive.

More importantly, fairness means that secondary uses of health information are not allowed, unless the data controller obtained the data subject's free and informed consent to the new use[28].

A second core principle of data protection laws is that there should be restrictions on the amount of personal data collected; the amount of data collection should be limited to what is necessary to achieve the purpose(s) for which the data are gathered and processed. The principle has been defined either as **principle of 'minimality',** 'necessity', 'non-excessiveness', or 'proportionality'[29].

As with the principle of fair and lawful processing, the principle of minimality is manifest in a variety of provisions. Art 6(1)(c) of the EC Directive on Data Protection, for instance, stipulates that personal data must be 'relevant and not excessive in relation to the purposes for which they are collected and/or further processed'. It is also manifest in provisions such as art 6(1)(e) of the Directive, which requires personal data to be erased or anonymised once they are no longer required for the purposes for which they have been kept. The minimality principle is further expressed in the Directive's basic regulatory premise — embodied in arts 7-8 — which state that the processing of personal data is prohibited unless it is necessary for achieving certain specified goals.

The minimality principle is not established so clearly in all data protection instruments as it does in the Directive. For instance, the 1990 UN Data Protection Guidelines (UN Guidelines) and the OECD Guidelines omit an express requirement of minimality at the stage of data collection, although such a requirement can, in principle could be inferred by the more general criterion of fairness. The OECD Guidelines also omit a specific provision on the destruction or anonymisation of personal data after a certain period. However, erasure or anonymisation may be obtained according to the principle of 'purpose specification', which is indeed clearly expressed in the OECD guidelines.

Another core principle of data protection laws is that personal data should be collected for specified, lawful and legitimate purposes and not subsequently be processed in ways that are incompatible with those purposes. This norm is often termed the **principle of 'purpose specification'**, 'purpose finality' or 'purpose limitation' [30].

The principle has three separate components, each of which may be regarded as a principle in it. Firstly, it means that the purposes for which data are collected should be specified/defined. Secondly, these purposes should be lawful/legitimate. Thirdly, the purposes for which the data are further processed should not be incompatible with the purposes for which the data are first collected. The norm imposes an obligation to data controllers to specify, from the design stage, the scope of the collection and processing of health data, and oversee any possible further use that

---

[28] This line has been taken by the UK Data Protection Tribunal. See especially the Tribunal's decision of 24.3.1998 in British Gas Trading Limited v Data Protection Registrar (case reference unspecified). Compare also National Privacy Principle 2.1(a)-(b) in Sch 3 to Australia's federal Privacy Act.

[29] This term is employed by the Council of Europe in several of its data protection instruments: see, for example, para 4.7 of Recommendation No R (97) 18 on the Protection of Personal Data Collected and Processed for Statistical Purposes (adopted 30 September 1997).

[30] See, for example, para 9 of the OECD Guidelines and Principle 3 of the UN Guidelines.

might subsequently come true. The requirement for purpose specification is envisaged in all of the main international data protection instruments[31].

Another fundamental principle is that of **information quality**, which is set forth in all data protection laws; although their wording, scope and stringency vary considerably. Article 5(d) of the CoE Convention and art 6(1)(d) of the EC Directive state that personal data shall be 'accurate and, where necessary, kept up to date'[32].

It means that personal data should be valid and accurate with respect to what they are intended to describe, and relevant and complete with respect to the purposes for which they are intended to be processed.

The **principle of subject participation and control** expresses the concept that individuals should participate and have a certain control over the processing of data concerning themselves. The individual participation principle, firstly established by section 13 of the OECD Guidelines, is indeed further and more specifically expressed in the EU Data Protection Directive. Arts 10-11 of the EC Directive, in summary, require data controllers to directly supply data subjects with basic information about the parameters of their data processing operations, independently of the data subjects' use of their own access rights. For example, individuals have to be informed of the identity of the controller, the purpose of the processing, the recipients of the data and the existence of the right to access and rectify data concerning him. None of the other main international data protection instruments lay down such requirements directly[33].

An exemption to the norm is provided by art. 11 (par. 2) of the EU Directive, which states that information to the data subject may not be supplied in the processing of data for statistical, historical and scientific research purposes, where the provision of such information proves impossible or would involve a disproportioned effort.

In this case, the interest in the individual's privacy protection has been balanced with public interests of society.

The principle of control is clearly expressed by two norms of the EU Directive, namely art. 12 and 14, which established the data subject rights to access to data and to object.

---

[31] See art 5(b) of the CoE Convention, art 6(1)(b) of the EC Directive, Principle 3 of the UN Guidelines and para 9 of the OECD Guidelines.

[32] Identical or near-identical requirements are set down in the provisions of several national laws, including art 9(1)(c) of Italy's Law on Protection of Individuals and Other Subjects with Regard to Processing of Personal Data and Data Protection Principle 4 in Sch 1 to the 1998 UK legislation.

[33] The UN Guidelines' 'principle of purpose specification' (principle 3) stipulates that the purpose of a computerised personal data file should 'receive a certain amount of publicity or be brought to the attention of the person concerned'. Compare the more generally formulated 'Openness Principle' in para 12 of the OECD Guidelines: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller. Articles 10-11 of the Directive are supplemented by art 21 which requires member states to 'take measures to ensure that processing operations are publicised' (art 21(1)) and to ensure that there is a register of processing operations open to public inspection (art 21(2)

An influential formulation of this right is given in art 12 of the EC Directive, which provides individuals with a right of access not just to data relating directly to them but also to information about the way in which the data are used, including the purposes of the processing, the recipients and sources of the data, and the 'logic' involved in certain automated data processing operations.

The right of access also implies the data subject's capability to obtain the erasure or blocking of the processing of data that are not compliant with the provision of the Directive, in particular because of the incomplete or inaccurate nature of data. Moreover, any rectification, erasure or blocking carried out in accordance to art. 12 (b), has to be notified to the eventual third parties to whom the data have been disclosed.

With respect to rectification rights, most data protection instruments have provisions, which give persons the right to demand that incorrect, misleading or obsolescent data relating to them be rectified or deleted by those in control of the data, and/or require that data controllers rectify or delete such data[34]. None of them, however, come into details as the Directive does.

Exceptions are provided by art. 13 of the Directive, which, among the others, limits the subject's right to access when, subject to legal safeguards provided by domestic laws, "data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics".

The right in art 12 is similar to, but more extensive than, the equivalent rights found in the other main international data protection instruments[35]. None of the latter, with the exception of the UN Guidelines, specifically mentions the subject's right to be informed of the recipients of data. None mention the right to be informed of the logic behind automated data processing.

Another important sub-principle of control is the right to object to others' processing of data on themselves and the right to demand that invalid, irrelevant or illegally data be corrected or erased.

The ability to object is linked primarily to rules prohibiting various types of data processing without the consent of the data subjects. Such rules are especially prominent in the EC Directive, where consent is a pre-requisite to any processing. It is important to note that consent is rarely laid down as the sole precondition for the particular type of processing in question; consent tends to be one of several alternative prerequisites. This is also the case with the EC Directive. The alternative prerequisites are often broadly formulated, significantly reducing the extent to which data controllers are hostage to the consent requirement in practice.

A specific right to object is also laid down in some data protection laws. The EC Directive contains important instances of such a right:

Art 14(a), provides a right to object to data processing in some circumstances referred to in art 7 (e) and (f); however, it can be inferred that the right to object cannot be exerted when the processing is considered legitimate according to art. 7 of the Directive.

---

[34] See for example art 12(b) of the EC Directive, Principle 4 of the UN Guidelines, s 14 of the UK Act, art 13(1)(c) of the Italian Act.

[35] See art 8 of the CoE Convention, paras 12-13 of the OECD Guidelines and principle 4 of the UN Guidelines.

Art 14(b) establishes a general right to object to the processing for the purposes of direct marketing.

Most innovatively, art 15(1) stipulates a right to object to decisions based on fully automated assessments of one's personal character.

These rights to object are not found in the other main international data protection instruments.

In general, disclosure of data to third parties may occur only if certain conditions are met: for example, consent of the data subject has been obtained, or disclosure is provided by the authority of law"[36].

Neither the CoE Convention nor the EC Directive specifically address the issue of **disclosure limitation**, since the issue is disciplined by the norms related to the conditions for the legitimate processing of data[37]. Thus, neither of these instruments recognise disclosure limitation as a separate principle but incorporate it within other principles, particularly those of fair and lawful processing, and purpose specification. The EU model of data protection, in fact, enhances general and abstract laws that govern the handling of personal information in a univocal manner, from collection to processing and disclosure.

The OECD Guidelines incorporate the principle of disclosure limitation within a broader principle termed the 'Use Limitation Principle' (para 10), while the UN Guidelines specifically address the issue of disclosure under the principle of purpose specification.

Nevertheless, disclosure limitation, outside the EU, is regarded as a principle in its own and numerous national statutes expressly delineate it as a separate principle or set of rules[38].

The **principle of information security** stipulates that data controllers should take steps to ensure that personal data are not destroyed accidentally or subject to unauthorised access, alteration, destruction or disclosure. Representative provisions to this effect are art 7 of the CoE Convention and art 17 of the EC Directive.

The **principle of sensitivity** stipulates that the processing of data, which are especially sensitive for data subjects, should be subject to more stringent controls than other data.

The principle is primarily manifest in rules that place special limits on the processing of predefined categories of data. The most influential list of these data categories is provided in art 8(1) of the EC Directive, which includes 'racial or ethnic origin', 'political opinions', 'religious or philosophical beliefs', 'trade union membership', 'health' and 'sexual life'.

Further, art 8(5) makes special provision for data on criminal records and the like. Similar lists are found in other data protection instruments at both international and national level, but these vary somewhat in scope. For instance, the list in art 6 of the CoE Convention omits data on trade union membership, while the list in the UN Guidelines includes data on membership of associations in general (not just trade unions).

---

[36] Paragraph 10 of the OECD Guidelines

[37] See especially arts 5(a), 5(b) and 6 of the Convention, and arts 6(1)(a), 6(1)(b), 7 and 8 of the Directive

[38] See for example the US federal Privacy Act (5 USC s 552a(b)-(c)), s 8 of Canada's federal Privacy Act, and Information Privacy Principle 11 in both the NZ Privacy Act and Australia's federal Privacy Act.

A common assumption in data protection discourse is that the sensitivity of data depends on the context in which the data are used. Accordingly, attempts to single out particular categories of data for special protection independent of their context has not been without controversy.

3.7 The privacy legal framework in the context of the BIRO project

The BIRO Information System involves the use of sensitive-medical data collected through diabetes registries within national boundaries and further processed for public health studies at international level.

Hence, the following legislation and guidelines are, in principle, applicable to BIRO:

1. *EU legislation:*
    - Directive 95/46/EC (Data Protection Directive)
    - Directive 2002/58/EC (Telecommunication Directive)
    - Treaty of the European Union (Art. F)
    - Convention Protection of Human Rights (Art. 8)
    - Charter of Fundamental Rights (Art. 8)
2. *Council of Europe:*
    - Convention 108/88;
    - Recomm. R(99)5 & R(97)5
    - Convention on Biomedicine(1997)
3. *OECD:*
    - Guidelines on Security of Information Systems
    - Guidelines on Privacy
4. *United Nations:*
    - Universal Declaration of Human Rights (Art XII);
    - UN Guidelines on computerized personal data file;
    - Int. Covenant on Civil and Political Rights (Art. 17)

In the context of the BIRO project, however, only some of the norms contained in the aforementioned legislation, international agreements and guidelines are directly applicable.

It has to be noted that the collection of data take place at national level; and the investigation of privacy compliance of registries is out of the scope of the present report, nor it will be assessed in the final privacy impact assessment.

The privacy analysis will cover any privacy issue that might arise in the transfer of data from the BIRO Centres to the central database, hosted by the University of Perugia, Italy.

It can be asserted, at a general level, that the kind of processing that takes place in the BIRO Centres is subject to art. 8 (par. 3) of the Data Protection Directive.

Each centre collects information relating to an identified or identifiable natural person for the purpose of setting up diabetes registries. Hence, it can be inferred that those data are collected and processed for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health care services. According to the EU Data Protection Directive, consent from the data subject may not be required in this case. The norm constitutes an exemption to the prohibition of processing sensitive data, which are set up by art. 8 of the Directive, justified by the need to guarantee the fulfilment of the competing interest of societies to a better health care. Domestic laws may provide more stringent rules though.

Each centre of the BIRO consortium provides for the anonymisation of data before transferring them to the BIRO central database, where they will be processed for statistical and scientific purposes. Aggregated data are inherently anonymised.

The further processing of personal data for statistical or scientific research purposes is generally considered, within the EU Directive, compatible with the purposes for which the data have previously being collected. This principle is expressed, among the others, in the provision of art. 11, par. 2 of the EU Directive.

While art. 10 and 11 impose to data controller, as a general rule, to give some kind of information to the data subject - for instance, the right to know the identity of the controller, the purpose of the processing and any further information - paragraph 2 of art. 11 exempts the data controller from providing such information when the processing is performed for statistical or scientific research purposes, if the provision of such information proves impossible or would involve a disproportionate effort.

The case of BIRO falls within the scope of the latter case (art 11, par. 2). Consequently, the information that usually the data controller has to provide to the data subject (patient) could be waived if the circumstances described verify (that is: when the provision of such information proves impossible or would involve a disproportionate effort), unless domestic law provides differently.

The exemptions provided by the Directive are also in line with the Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data (1981), which envisages the possibility of restricting the exercise of the data subject's rights with regard to data processing operations that pose no risk (art. 9, par. 3). Examples of no or minimal risk operations are, in particular, the use of data for statistical work, in so far as those data are presented in aggregate form and stripped of their identifiers. Similarly, scientific research is included in this category.

It is worth noting that the single centres of the consortium will be instead subject to the other general rules and principles imposed by the Directive and by other international legal instruments:

Hence, personal data collected in the registries have to be:

a) processed fairly and lawfully;

b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes

c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed

d) accurate and, where necessary, kept up to date

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.processed by a health professional subject under national law or rules to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy medical data will be kept no longer than necessary to achieve the purpose for which they were collected and processed

h) medical data used for scientific research purposes will be anonymous and not published in a form which enables the data subjects to be identified.

In addition, they have to guarantee the subject's right to access his/her data, the right to rectification, erasure or blocking of data which are either processed not in compliance with the Directive, or are incomplete, inaccurate or erroneous. The subject's right to objects has also to be warranted, if based on compelling legitimate grounds relating to the data subject's particular situation. Confidentiality issues have to be addressed according to art. 16 of the Directive and, most importantly, security requirements have to be complied with.

The fulfilment of the above requirements is a matter of domestic investigation, which is, as previously announced, outside the scope of the present investigation. The privacy analysis provided is rather intended to be a checklist or a framework for those partners of the BIRO project who are still undergoing the setting up of their diabetes registries or are revising them; so that their conformity to the relevant EU legislation will be ensured.

As far as transborder data flow is concerned, it can be asserted that the free flow of information, regardless of frontiers, is a principle enshrined in Article 10 of the European Human Rights Convention. Accordingly, art 12 of the Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) and art. 25 of the EU Data Protection Directive (1995) discipline the transfer of data from one country to another.

The main rule contained in art 12 (paragraph 2) of the Convention, is that, in principle, obstacles to transborder data follows are not permitted between Contracting States in the form of prohibitions or special authorisations of data transfers. The rationale for this provision is that all Contracting States, having subscribed to the common core of data protection provisions set out in Chapter II, offer a certain minimum level of protection.

In addiction, art 12 (2) states that prohibiting or subjecting to special authorizations transborder flows of personal data, is allowed only "for the sole purpose of the protection of privacy". The norm adds an important clarification, namely that a Contracting State may not invoke this convention to justify interference with transborder data flows for reasons which have nothing to do with the protection of privacy.

However, paragraph 2 of this article does not affect the possibility for a Party to lay down in its domestic data protection law provisions, which, in particular cases do not permit certain transfers of personal data, irrespective of whether such transfers take place within its territory or across the borders.

The Council of Europe Recommendation on the Protection of Medical Data, resembles the Convention and establishes that the transborder flow of medical data to a state which has ratified the Convention for the Protection of Individuals with regard to Automatic Processing of Personal

Data, and which disposes of legislation which provides at least equivalent protection of medical data, should not be subjected to special conditions concerning the protection of privacy.

Where the protection of medical data can be considered to be in line with the principle of equivalent protection laid down in the convention, no restriction should be placed on the transborder flow of medical data to a state which has not ratified the convention, but which has legal provisions which ensure protection in accordance with the principles of that convention and the recommendation.

Unless otherwise provided for by domestic law, the transborder flow of medical data to a state which does not ensure protection in accordance with the convention and with this recommendation, should not as a rule occur, unless necessary measures, including those of a contractual nature, to respect the principles of the convention and this recommendation, have been taken, and the data subject has the possibility to object to the transfer; or the data subject has given his consent.

According to the EU Directive, the cross border flows of personal data are allowed only when an adequate level of privacy protection is envisaged in the countries involved in the processing operations.

Following the same reasoning applied to the interpretation of the Convention, countries that have implemented the Directive are automatically allowed to transborder data flows: complying with the Directive ensures, “ipso iure”, an adequate level of protection.

The Centres involved in the BIRO project belong to European countries that have fully implemented the EU Data Protection Directive, and ratified the Convention; hence, an adequate level of privacy protection is fully guaranteed across the countries involved. This means that the exchange of data envisaged in the project is legally viable, according to EU legislation.

4. Description of Personal Information & Data Flow

4.1 Data Collection

The prospective number of patients that will be initially included in the BIRO project is 115,000 (except for Norway and Romania that still need to communicate figures). The cohort is composed as follow:

- Umbria: 30,000 patients
- Tayside: 15,000 patients
- Styria+Carinthia: 40,000 patients
- Cipro: 5,000 patients
- Malta: 25,000 patients

4.2 The BIRO Architecture & Data Flow

The BIRO activity starts by formatting data for further manipulation. Each partner will prepare a "BIRO data export" in order to allow the mapping of centres' data to a BIRO compliant dataset. The resulting transfer files will be loaded into a DBMS (WP6) through a specialised application developed for the scope. The DBMS will then be used to process data either directly, or in combination with the statistical engine (WP8).

A set of procedures will be used to carry out mathematical computations required to output a set of summary parameters (statistical objects) that will be then transmitted to a central server via specialised communication software (WP9). The server hosts the central engine (WP10). The engine will comply with specifications given by the Report Templates (WP7) to produce a range of outputs that will be stored using different formats, as required.

Figure 1 describes the BIRO architecture and software requirements. Figure 2 describes the BIRO personal information and data flow.

4.3 Early Identification of BIRO Candidate Alternative Architectures

BIRO partners identified three alternatives for building up the BIRO Information System:

a) *Individual Patients, De-identified (Pseudonym):* In this case there will be a need to specify secure patient's identity encryption algorithm and privacy protective technology for securing the data transfer.

b) *Aggregation by group of patients, Centre ID Available (De-identified):* The use of aggregated data, instead, will require the specification of secure encryption algorithm for Centre identity and privacy protective technology for securing the data transfer

c) *Aggregation by region:* Finally, in the aggregation of data by region there is a need to specify optimised data aggregation in order to impede reverse engineering. Privacy protective technology should be used for securing the data transfer.

5. Potential privacy risks

Potential privacy risks will be analysed through summary tables, which will allow estimating the better privacy protective alternative in the processing of the data gathered.

An example of summary table is provided below (see Table 1). The level of risk will be classified as follows:

- Low: There is a possibility that the risk will materialize but there are mitigating factors.
- Moderate: There is a strong possibility that the risk will materialize if no corrective measures are taken.
- High: There is a near certainty that the risk will materialize if no corrective measures are taken.

Table 1

Example of a Summary Table

Element	Nature of risks	Level of risks			Comments	Mitigating Mechanisms
		Low	Medium	High		
Individual data	Individual privacy			X	Pose a direct risk to individual's privacy	Non-Reversible De-identification
Aggregated data	Individual privacy		X		Pose an indirect risk to individual's privacy	Non-reversible De-identification

In all cases described above, the BIRO Information System will process only de-identified data. Hence the level of risk will be necessarily very low.

Nevertheless, it is crucial to foresee any possible breach of privacy through the adoption of appropriate technologies ensuring that encryption algorithms will be efficient and produce a secure environment for the data processed. For instance, it is fundamental to guarantee that reverse engineering will be impeded through appropriate mechanisms.

It has to be pointed out that, at this stage, a true analysis of the privacy risks cannot be performed, since the BIRO architecture and data flow are yet to be defined. Hence, the analysis of privacy risks will be provided through a separate report in step 3 of the privacy impact assessment.

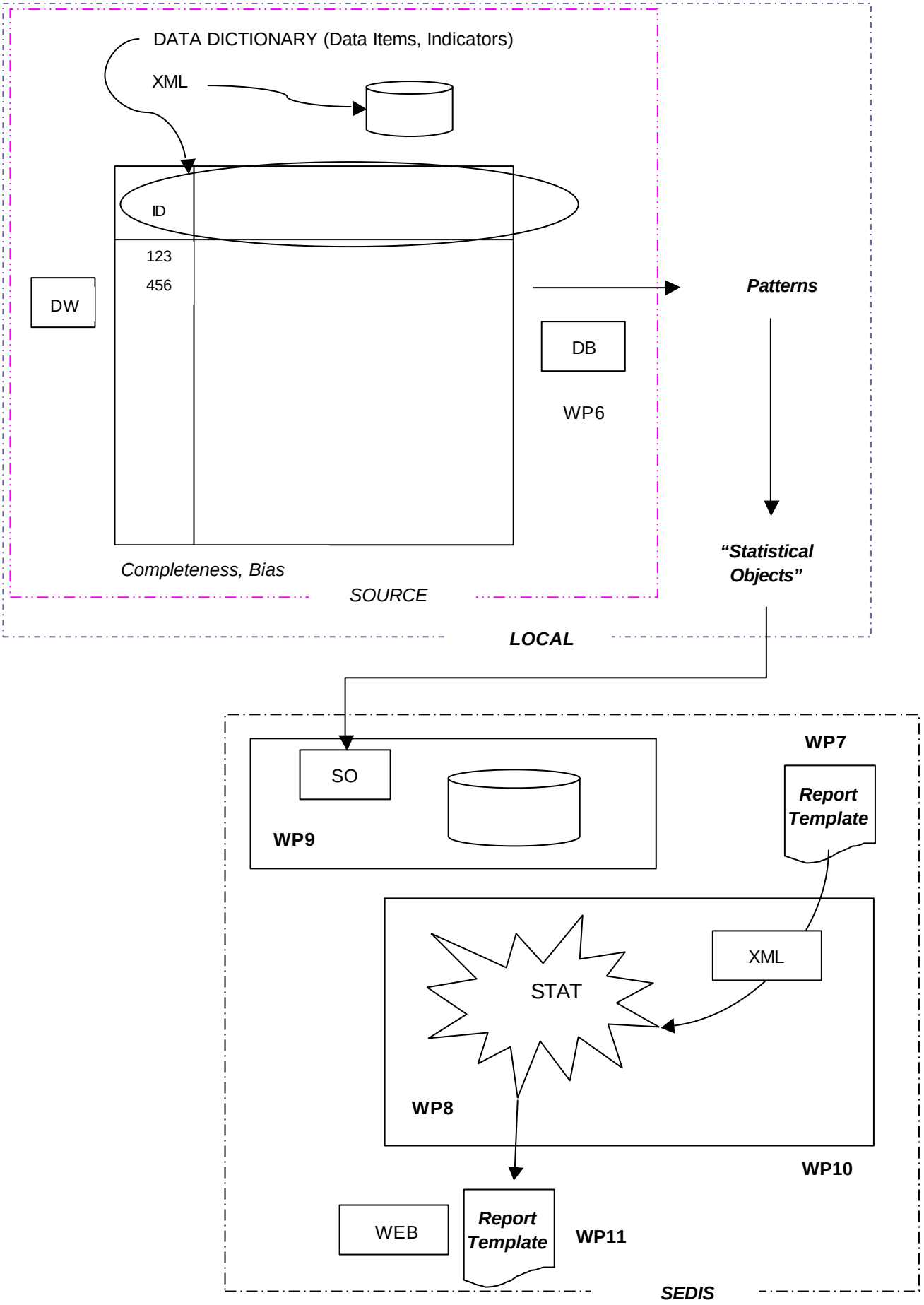
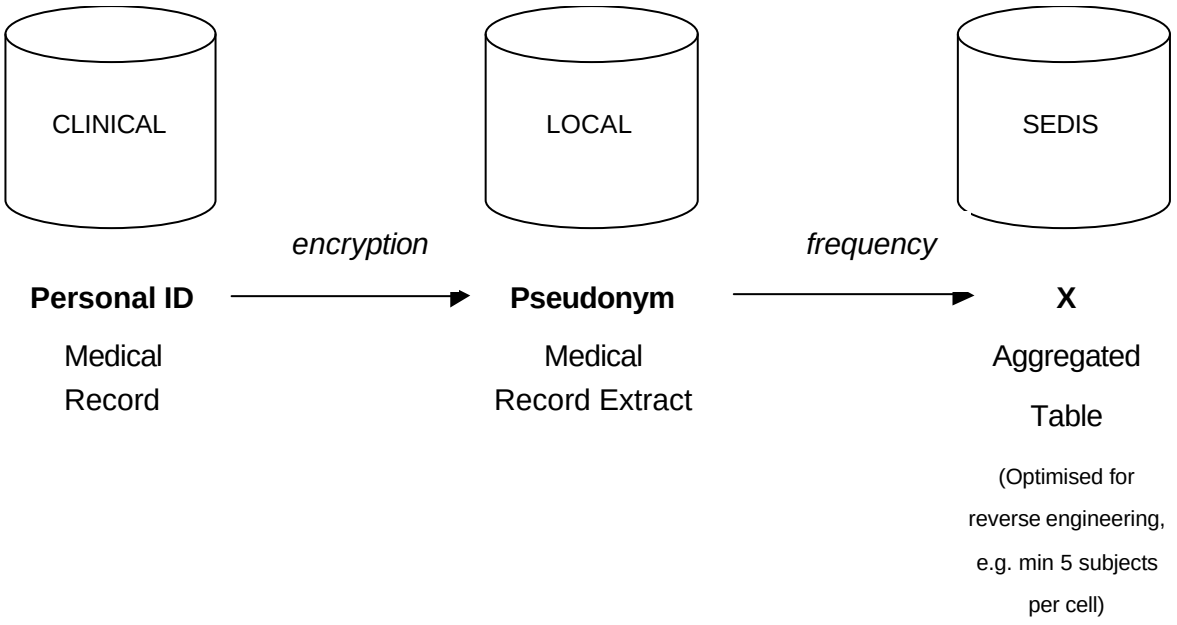


Fig.1 BIRO Architecture and Software Requirements

Fig. 2. BIRO PERSONAL INFORMATION AND DATA FLOW



6. Overview of Security Requirements

The BIRO project is subject to the following principles and requirements in the implementation of the Diabetes Information System[39]:

1. Appropriate technical and organisational measures have to be taken to protect personal data against:
   - accidental or illegal destruction
   - accidental loss
   - unauthorised access or alteration
   - communication or any other form of processing
2. Such measures have to ensure an appropriate level of security taking into account:
   - the technical state of the art
   - the sensitive nature of medical data
   - the evaluation of potential risks

[39] Art 9 of the Council of Europe Recommendation No R (97) 5 on the Protection of Medical data

3. These measures are to be reviewed periodically.
4. In particular, to ensure the privacy, confidentiality, integrity and accuracy of processed data, as well as the protection of patients, appropriate measures have to be taken:to prevent any unauthorised person from having access to installations used for processing personal data (**control of the entrance to installations**);

   b) to prevent data media from being read, copied, altered or removed by unauthorised persons (**control of data media**);

   c) to prevent the unauthorised entry of data into the information system, and any unauthorised consultation, modification or deletion of processed personal data (**memory control**);

   d) to prevent automated data processing systems from being used by unauthorised persons by means of data transmission equipment (**control of utilisation**); with a view to, on the one hand, selective access to data and, on the other hand, the security of the medical data, to ensure that the processing as a general rule is so designed as to enable the separation of:

      - identifiers and data relating to the identity of persons;
      - administrative data;
      - medical data;
      - social data;
      - genetic data (**access control**);

   e) to guarantee the possibility of checking and ascertaining to which persons or bodies personal data can be communicated by data transmission equipment (**control of communication**);

   f) to guarantee that it is possible to check and establish “a posteriori” who has had access to the system and what personal data have been introduced into the information system, when and by whom (**control of data introduction**);

   g) to prevent the unauthorised reading, copying, alteration or deletion of personal data during the communication of personal data and the transport of data media (**control of transport)**;

   h) to safeguard data by making security copies (**availability control**)

In order to implement the above security requirements a set of techniques have so far been identified by the Italian legislation through a technical Annex (Annex B) to the Italian Data Protection Code[40], which is relative to technical specifications concerning minimum security

[40] Decreto legislativo 30 giugno 2003, n. 196, CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI, aggiornato alla legge 12 luglio 2006, n. 228 di conversione, con modificazioni, del decreto-legge 12 maggio 2006, n. 173. Available at:

measures.

Since the BIRO project will develop a database, SEDIS, to be hosted in the University of Perugia, Italy, the Italian legislation has to be complied with. The data controller, data processor – if nominated – and person(s) in charge of the processing will implement the following technical arrangements:

Computerised Authentication System

1. Persons in charge of the processing are allowed to process personal data by electronic means if they are provided with authentication credentials such as to successfully complete an authentication procedure relating either to a specific processing operation or to a set of processing operations.

2. Authentication credentials consist in an ID code for the person in charge of the processing, as associated with a secret password that shall only be known to the latter person; alternatively, they consist in an authentication device that shall be used and held exclusively by the person in charge of the processing and may be associated with either an ID code or a password, or else in a biometric feature that relates to the person in charge of the processing and may be associated with either an ID code or a password.

3. One or more authentication credentials have to be assigned to or associated with each person in charge of the processing.

4. The instructions provided to the persons in charge of the processing has to lay down the obligation to take such precautions as may be necessary to ensure that the confidential component(s) in the credentials are kept secret and that the devices used and held exclusively by persons in charge of the processing are kept with due care.

5. Where provided for by the relevant authentication system, a password shall consist of at least eight characters; if this is not allowed by the electronic equipment, a password shall consist of the maximum permitted number of characters. It shall not contain any item that can be easily related to the person in charge of the processing and shall be modified by the latter when it is first used as well as at least every six months thereafter. If sensitive or judicial data are processed, the password shall be modified at least every three months.

6. An ID code, if used, may not be assigned to another person in charge of the processing even at a different time.

7. Authentication credentials shall be de-activated if they have not been used for at least six months, except for those that have been authorised exclusively for technical management purposes.

8. Authentication credentials shall be also de-activated if the person in charge of the processing is disqualified from accessing personal data.

---

http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Normativa%2FItaliana%2FII+Codice+in+materia+di+protezione+dei+dati+personali

9. The persons in charge of the processing shall be instructed to the effect that electronic equipment should not be left unattended and made accessible during processing sessions.

10. Where data and electronic equipment may only be accessed by using the confidential component(s) of the authentication credential, appropriate instructions shall be given in advance, in writing, to clearly specify the mechanisms by which the data controller can ensure that data or electronic equipment are available in case the person in charge of the processing is either absent or unavailable for a long time and it is indispensable to carry out certain activities without further delay exclusively for purposes related to system operationality and security. In this case, copies of the credentials shall be kept in such a way as to ensure their confidentiality by specifying, in writing, the entities in charge of keeping such credentials. Said entities shall have to inform the person in charge of the processing, without delay, as to the activities carried out.

11. The provisions concerning the authentication system referred to above as well as those concerning the authorisation system shall not apply to the processing of personal data that are intended for dissemination.

Authorisation System

12. Where authorisation profiles with different scope have been set out for the persons in charge of the processing, an authorisation system shall be used.

13. Authorisation profiles for each person or homogeneous set of persons in charge of the processing shall be set out and configured prior to start of the processing in such a way as to only enable access to the data that are necessary to perform processing operations.

14. It shall be regularly verified, at least at yearly intervals, that the prerequisites for retaining the relevant authorisation profiles still apply.

Other Security Measures

15. Within the framework of the regular update – to be performed at least at yearly intervals – of the specifications concerning the scope of the processing operations that are entrusted to the individual persons in charge of the processing as well as to the technicians responsible for management and/or maintenance of electronic equipment, the list of the persons in charge of the processing may also be drawn up by homogeneous categories of task and corresponding authorisation profile.

16. Personal data shall be protected against the risk of intrusion and the effects of programmes as per Section 615-quinquies of the Criminal Code by implementing suitable electronic means to be updated at least every six months.

17. The regular update of computer programmes as aimed at preventing vulnerability and removing flaws of electronic means shall be carried out at least annually. If sensitive or judicial data are processed, such update shall be carried out at least every six months.

18. Organisational and technical instructions shall be issued such as to require at least weekly data back-ups.

Security Policy Document

19. By 31 March of each year, the controller of processing operations concerning sensitive and/or judicial data shall draw up, also by the agency of the data processor, if nominated, a security policy document containing appropriate information with regard to:

19.1 the list of processing operations concerning personal data,

19.2 the distribution of tasks and responsibilities among the departments/divisions in charge of processing data,

19.3 an analysis of the risks applying to the data,

19.4 the measures to be taken in order to ensure data integrity and availability as well as protection of areas and premises insofar as they are relevant for the purpose of keeping and accessing such data,

19.5 a description of the criteria and mechanisms to restore data availability following destruction and/or damage as per point 23 below,

19.6 a schedule of training activities concerning the persons in charge of the processing with a view to informing them on the risks applying to the data, the measures that are available to prevent harmful events, the most important features of personal data protection legislation in connection with the relevant activities, the resulting liability and the arrangements to get updated information on the minimum security measures adopted by the data controller.

Said training activities shall be planned as of the start of the employment relationship as well as in connection with changes in the task(s) discharged and/or the implementation of new, significant means that are relevant to the processing of personal data,

19.7 a description of the criteria to be implemented in order to ensure adoption of the minimum security measures whenever processing operations concerning personal data are externalised in accordance with the Code,

19.8 as for the personal data disclosing health and sex life referred to under point 24, the specification of the criteria to be implemented in order to either encrypt such data or keep them separate from other personal data concerning the same data subject.

Additional Measures Applying to Processing of Sensitive Data

20. Sensitive or judicial data shall be protected against unauthorised access as per Section 615-ter of the Criminal Code by implementing suitable electronic means.

21. Organisational and technical instructions shall be issued with regard to keeping and using the removable media on which the data are stored in order to prevent unauthorised access and processing.

22. The removable media containing sensitive or judicial data shall be destroyed or made unusable if they are not used; alternatively, they may be re-used by other persons in charge of the processing, who are not authorised to process the same data, if the information previously contained in them is not intelligible and cannot be re-constructed by any technical means.

23. If either the data or electronic means have been damaged, suitable measures shall be

adopted to ensure that data access is restored within a specific deadline, which must be compatible with data subjects' rights and not in excess of seven days.

24. Health care bodies and professionals shall process data disclosing health and sex life as contained in lists, registers or data banks in accordance with the mechanisms referred to in Section 22(6) of the Code also in order to ensure that said data are processed separately from the other personal data allowing data subjects to be identified directly. Data concerning genetic identity shall only be processed in protected premises that may only be accessed by such persons in charge of the processing and entities as have been specifically authorised to access them. Containers equipped with locks or equivalent devices shall have to be used in order to remove the data outside the premises reserved for their processing; the data shall have to be encrypted for the purpose of electronically transferring them.

Safeguards and Protections

25. Where a data controller adopts minimum security measures by committing the relevant tasks to external entities, prior to implementing such measures he or she shall require the installing technician(s) to supply a written description of the activities performed by which it is certified that they are compliant with the provisions set out in these technical specifications.

26. The circumstance that the security policy document has been drawn up and/or updated shall be referred to in the management report that the data controller may be required to submit together with the relevant balance sheet.

7. PIA Plan

The PIA process will include 4 steps:

Step 1: Preliminary PIA

Step 2: Data flows Analysis

Step 3: Privacy analysis

Step 4: PIA Report

In Step one, the Privacy Impact Assessment Team has been designated. The objectives of the preliminary PIA are to highlight significant privacy risks in the management of the BIRO Information System and to identify the main alternatives for the development of BIRO through a review of the literature.

The literature review has allowed identifying a checklist of key privacy requirements/criteria to which the BIRO Information System shall be compliant with.

In addiction, a limited number (N=3) of candidate alternative architectures have been selected by all partners taking into account both the respect of privacy principles, legislation, regulations, guidelines and rules, and the best performance of the BIRO Information System.

The Preliminary PIA Report has been delivered at the end of the first phase.

In step two there will be a detailed description of the personal information flow and an in-depth analysis of the selected alternatives. The purpose of this step will be to produce a definitive ranking of the selected alternatives. To this end, information flow diagrams, data flow tables and a panel ranking form will be used.

In synthesis, the PIA Team will evaluate each alternative against the privacy criteria agreed in step 1, including technology issues. A consensus panel (modified Delphi Panel) will be set up to rank the best privacy protective alternative: a mark will be assigned to each privacy criterion and all alternatives will be evaluated against the same privacy criteria/requirements. Consequently, the best scoring alternative will identify the best privacy enhancing system architecture. A Data Flow Report will be delivered at completion of this second phase.

In the Third Step, the data flows of the selected alternative will be examined in the context of applicable privacy policies and legislation.

The privacy analysis will derive from yes/no responses to a series of privacy related questions, sourced by a questionnaire, specifically produced for the purposes of the BIRO project by the PIA Team. The questionnaire will be used to facilitate the identification of major privacy risks and vulnerabilities of the selected BIRO architecture.

In order to measure privacy risks and vulnerabilities, the three dimensional privacy metrics will be used:

- Identity, which measures the degree to which information is personally identifiable. The Identity measurement takes place on a continuum, from full anonymity (the state of being without name) to full verinymity (being truly named).

- Linkability, which measures the degree to which data elements are linked to each other.
- Observability, which measures the degree to which identity or linkability may be impacted from the use of a system.

In terms of such metrics, the PIA goals are to minimize identity, linkability and observability.

Possible solutions for each privacy risk will be then developed and the BIRO partners will be able to revise the BIRO Information System accordingly. A Privacy Analysis Report will be also delivered.

In Step 4, the final Privacy Impact Assessment Report will be produced. The PIA Report will be a documented evaluation of the privacy risks and associated implications of the BIRO Information System, along with a discussion of possible remedies or mitigation strategies. It includes an accompanying action plan to ensure that privacy is managed effectively during the maintenance of the BIRO Information System.