Malta Meeting 2006

Applicability of EU privacy standards: an open question

1st BIRO Technology Transfer Workshop

Dr. Concetta Tania Di Iorio
Serectrix s.n.c.
E-mail: tania_diiorio@virgilio.it

The Right To Privacy

- **Privacy is a human right** generally recognized around the world and crystallised in many international instruments

- The **Universal Declaration of Human Rights (1950)** 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"

Other International and EU Instruments

- **Council of Europe's (1981) Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data**
- **OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data**, which set out specific rules covering the handling of electronic data
- Council of Europe **Convention on Cybercrime**
- **European Convention for the Protection of Human Rights and Fundamental Freedoms (1950)**
- **Charter of Fundamental Rights of the EU**
- **EU Directives:**
  - **Directive on Data Protection (95/46/EC**)
  - **Directive (2002/58/EC)** on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector

Privacy Principles Contained in International Instruments

A fundamental assumption that can be drawn from health privacy laws is that health information should be **"patient's centred":**

- *clinical data should only be used for the purposes of the patient's own health care, except in defined circumstances*

The right to privacy is not an absolute right: it can be weighted against matters that benefit society as a whole, as in the case of health research

Privacy Principles Contained in International Instruments (2)

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

Personal information must be:

- obtained fairly and lawfully
- used only for the original specified purpose adequate, relevant and not excessive to purpose, accurate and up to date
- accessible to the subject
- kept secure
- and destroyed after its purpose is completed

The Data Protection Directive: 95/46/EC

The Directive reinforced current data protection laws and 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 contained strengthened protections over the use of sensitive data

The Data Protection Directive (2)

- **Article 7 of the Directive** provides a set of criteria for ‘legitimate processing’ of personal information:

  *“Any processing of personal data has to take place, either with the **unambiguous consent** of the data subject (patient), 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**”.*

- More stringent conditions apply to the processing of special categories of sensitive data, such as medical data

Article 8 of the Directive: Sensitive Data

- **According to Article 8 (1) of the Directive**:

  "Member States shall prohibit the processing of personal data concerning health and other sensitive data".

- **This prohibition shall, according to Article 8 (2), not apply where**:

  a)the data subject has given his explicit **consent** to the processing of those data, or

  b)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

  c)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

  d)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 ….; or

  e)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.

Article 8 of the Directive: Sensitive Data (2)

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

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

b) 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.

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.

Council of Europe Recommendation No. R (97) 5 Medical Data

Respect for privacy:

- The respect of rights and fundamental freedoms, and in particular of the right to privacy, shall be guaranteed during the collection and processing of medical data.
- Medical data may only be collected and processed if in accordance with appropriate safeguards which must be provided by domestic law.
- In principle, medical data should be collected and processed only by health-care professionals, or by individuals or bodies working on behalf of health-care professionals.
- Individuals or bodies working on behalf of health-care professionals who collect and process medical data should be subject to the same rules of confidentiality incumbent on health-care professionals, or to comparable rules of confidentiality.

Collection and Processing of Medical Data

- Medical data shall be collected and processed fairly and lawfully and only for specified purposes
- Medical data shall in principle be obtained from the data subject
- Medical data may be collected and processed:
  - if provided for by law for **public health reasons** or another important public interest; or
  - if permitted by law for **preventive medical purposes or for diagnostic or for therapeutic purposes** with regard to the data subject or a relative in the genetic line; or…..
  - if the data subject or his/her legal representative or an authority or any person or body provided for by law has given his/her **consent** for one or more purposes, and in so far as domestic law does not provide otherwise
- If medical data have been collected for preventive medical purposes or for diagnostic or therapeutic purposes, they may also be processed for the management of a medical service operating in the interest of the patient

Information to the Data Subject

The data subject shall be informed of the following:

- 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.
- The data subject should be informed at the latest at the moment of collection.

Consent, Comunication, Access, Rectification

- **Consent** should be free, express and informed
- **Medical data shall not be communicated:**
  - unless other appropriate safeguards are provided by domestic law
  - medical data may only be communicated to a person who is subject to the rules of **confidentiality** incumbent upon a health-care professional
- **Rights of access**:
  - every person shall be enabled to have access to his/her medical data, either directly or through a health-care professional or
  - The information must be accessible in understandable form
  - Access to medical data may be refused, limited or delayed only if the law provides for this
- **Right to Rectification:**
  - The data subject may ask for rectification of erroneous data concerning him/her and
  - in case of refusal, he/she shall be able to appeal.

Security

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

Security Principles (1)

To ensure the confidentiality, integrity and accuracy of processed data, as well as the protection of patients, appropriate measures should be taken:

- to prevent any unauthorised person from having access to installations used for processing personal data (**control of the entrance to installations**);
- to prevent data media from being read, copied, altered or removed by unauthorised persons (**control of data media**);
- to prevent the unauthorised entry of data into the information system, and any unauthorised consultation, modification or deletion of processed personal data (**memory control**);
- to prevent automated data processing systems from being used by unauthorised persons by means of data transmission equipment (**control of utilisation**);
- the processing as a general rule is to be 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**);

Security Principles (2)

- 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**);
- 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**);
- 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);
- to safeguard data by making security copies (**availability)**

Scientific Research

- Whenever possible, **medical data** used for scientific research purposes **should be anonymous**.
- However, **if such anonymisation would make a scientific research project impossible**, and the project is to be carried out for legitimate purposes, **it could be carried out with personal data on condition that**:
  a) the data subject has given his/her informed consent for one or more research purposes; or
  b) disclosure of data for the purpose of a defined scientific research project concerning an important public interest has been authorised by the body or bodies designated by domestic law, but only if:
     - the data subject has not expressly opposed disclosure; and
     - despite reasonable efforts, it would be impracticable to contact the data subject to seek his consent; and
     - the interests of the research project justify the authorisation; or
  c) the scientific research is provided for by law and constitutes a necessary measure for public health reasons

Scientific Research (2)

- Subject to complementary provisions determined by domestic law, **health-care professionals** entitled to carry out their own medical research **should be able to use the medical data which they hold as long as the data subject has been informed** of this possibility and has not objected
- As regards any scientific research based on personal data, the **incidental problems**, including those of an ethical and scientific nature, **raised by respect of the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data should also be examined in the light of other relevant instruments**
- Personal data used for scientific research **may not be published in a form which enables the data subjects to be identified, unless:**
  - they have **given their consent** for the publication and
  - **publication is permitted by domestic law.**

Directive 95/46/EC: Definitions

Personal Data means:

"Any information relating to an identified or identifiable natural person (data subject)"

Identifiable Person:

"Is one 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 social identity"