B.I.R.O.

Best Information through Regional Outcomes

A European Public Health Project, DG-SANCO, 2005-2008

Privacy Impact Assessment

Checklist of Key Criteria

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

BIRO Graz Meeting, 29-30 September 2006

Privacy Impact Assessment

Main features:

- To highlight significant privacy risks in the management of the BIRO Information System
- To identify the main alternatives of the BIRO architecture
- To identify the most privacy protective alternative
- To employ possible remedies and mitigation strategies to privacy risks in the BIRO architecture
- To ensure that privacy is managed effectively during the maintenance of the BIRO information System

Step 1: Preliminary PIA Tasks (1)

- The privacy facilitator will deliver a Preliminary PIA Report by 1st December 2006 (a draft Preliminary PIA will be put on the BIRO forum shortly, open to comments. Amendments will be made accordingly)
- **The PIA report includes**:
  - Introduction/project background
  - Legislative and policy framework
  - Description of personal information (required level of data aggregation and data flow)
  - Potential privacy risks
  - Overview of security requirements
  - PIA plan
- Reminder: at least a summary description of personal information to be used and data flow is needed to perform this task

Step 1: Preliminary PIA Tasks (2)

- Review of the literature (core articles):
  - PIA team members should identify possible privacy protective criteria/requirements for the BIRO Information System
  - The privacy facilitator will merge all the applicable key criteria/requirements to produce a final checklist
  - The final checklist will be circulated among the PIA team members, open to comments/modifications

    Deadline: 15th October 2006
  - Agreed checklist made available on the BIRO forum
- Partners should:
  - Produce a summary description of personal information used in the project and BIRO data flow, to allow preparation of the Preliminary PIA Report. Deadline: 30th October 2006
  - select a limited number of BIRO candidate alternative architectures Deadline: ***30th November 2006***

Privacy Framework

***The BIRO Information System shall ensure compliance with the following applicable legislation/regulations*:**

- *EU legislation:*
  - Directive 95/46/EC (Data Protection Directive)
  - Directive 2002/58/EC (Telecommunication Directive)
  - Treaty of the European Union (Art. F)
  - EU Convention Protection of Human Rights (Art. 8)
  - EU Charter of Fundamental Rights (Art. 8)
- *Council of Europe:*
  - Convention 108/88;
  - Recomm. R(99)5 & R(97)5
  - Convention on Biomedicine(1997)
- *OECD:*
  - Guidelines on Security of Information Systems
  - Guidelines on Privacy
- *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)

Privacy Checklist

The checklist is composed of two sets of criteria/requirements:

- Privacy & Health Information, which includes:
  - Compliance to general privacy principles
  - Compliance to specific privacy regulations related to health research, health care, registries, health data collections and information systems
- IT Functions & Security, which includes:
  - Application of privacy enhancing technologies
  - Compliance to security requirements set up by EU and international legislation/regulations/guidelines

Privacy Checklist Criterion Class 1

Privacy & Health Information Criteria

Data Quality

Personal data must be:

- processed fairly and lawfully;
- collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes
- adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed
- accurate and, where necessary, kept up to date
- 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

Criteria for Making the Data Processing Legitimate

Personal data may be processed only if:

- the data subject has unambiguously given his **consent** (this consent should be free, express and informed);
- it is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and
- those data are **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 (confidentiality)

Information of the data subject

The data subject has to 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;
- 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 & Communication

- 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 & Right to Rectification

Right to 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.

Criteria/requirements specifically related to 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**:
  - the data subject has given his/her informed consent for one or more research purposes; or
  - 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
- 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**

Privacy Checklist Criterion Class 2

IT Functions & Security

Security (1)

- **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 (2)

Measures to ensure the confidentiality, integrity and accuracy of processed data, as well as the protection of patients, should focus on:

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

Security (3)

- **control of communication:** to guarantee the possibility of checking and ascertaining to which persons or bodies personal data can be communicated by data transmission equipment;
- **control of data introduction:** 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 transport: to prevent the unauthorised reading, copying, alteration or deletion of personal data during the communication of personal data and the transport of data media
- **availability control:** to safeguard data by making security copies
- **Conservation:** In general, medical data shall be kept no longer than necessary to achieve the purpose for which they were collected and processed.