B.I.R.O

WP5: PRIVACY IMPACT ASSESSMENT (PIA)

PIA Article:

"PRIVACY IMPACT ASSESSMENT IN THE BIRO PROJECT: A NOVEL METHOD TO EMBED ETHICS AND SECURITY IN THE DESIGN OF COMPLEX HEALTH INFORMATION SYSTEMS "

ROMA MEETING

(20–21 APRIL 2008)

Concetta Tania Di Iorio
Serectrix snc
Tania_diiorio@virgilio.it

Article’s Structure

Abstract

1. Background
2. Materials and Methods
3. Results
4. Discussion
5. Conclusions

Background

Issues considered:

- Information technology and the right to privacy
- Public health and “Population-based Health Information Systems” need to access data from different sources: increasing demand for “Secondary uses” of health information
- The BIRO approach
- Health registries and databases
- Necessity to balance patients’ rights with the benefit of society toa better health
- PIA as a tool to provide efficient health information systems while guaranteeing the respect of privacy principles and concerns

Materials & Methods (1)

The BIRO project:

- General features of the BIRO project
- General objectives of BIRO
- Technology associated to SEDIS
- The overall model
- The level of aggregation: trade-off between
  - formal agreement
  - Legislation
  - Practical limits

Materials & Methods (2)

Design of The Privacy Impact Assessment:

- The PIA process:
  - Step 1: Preliminary PIA
  - Step 2: Data Flow Analysis
  - Step 3: Privacy Analysis
  - Step 4: PIA Report
- PIA main achievements:
  - Legislative review and summary evaluation of potential privacy risks
  - Selection of three alternative architectures for the BIRO information system
  - Data flow analysis
  - Modified Delphi procedure: identification of the best privacy protective BIRO system architecture

Materials & Methods (3)

The PIA process:

- BIRO Draft Diagram:
  - documents the general BIRO infrastructure architecture, the general flow of information through the system, any physical or logical separation of personal information/data, security mechanisms. Thus, it describes the general broad structure of the SEDIS information system
- Identification of three alternative architectures
  - literature review on privacy, privacy in disease registries and security)

Materials & Methods (4)

Data Flow Tables:

- Are specific tools developed in order to in depth describe and detail the dynamics involved in both data collection and information exchange procedures.

- The data flow tables of the three BIRO selected alternatives identify:
  - any cluster of personal information/data involved in BIRO System,
  - describe all personal data elements associated with the proposed system,
  - describe the collection, use and disclosure of personal information/data in the BIRO project and
  - list the different options available for data collection and exchange in each BIRO candidate architecture up to data disposition

Materials & Methods (5)

Data Flow Questionnaire & the Delphi Procedure:

- Information content of the questionnaire sourced by the data flow tables
- developed in the context of a **modified Delphi procedure**, whose results allowed the ranking of the candidate architectures
- The various options were discussed and grouped to specify the different solutions available for the definition of the final structure of the BIRO information system through a Delphi prodedure:
  - Anonymous phase
  - Consensus session
- The questionnaire provided a series of scenarios and, within each scenarios different sub-options have been identified, to which marks have been assigned on the basis of standard criteria (composite scoring) :
  - privacy
  - information content and
  - technical complexity
- The best BIRO architecture is a trade-off between higher levels of privacy protection, relevance of information content in relation to target diabetes indicators and the employment of minimal technical complexity

Results (1)

- Identification of three alternative architectures:
  - Individual Patients Data, de-identified through a pseudonym
  - Aggregation by Group of Patients, centre IDs available, but de-identified
  - Aggregation by Region
- Selection of the best BIRO architecture at conclusion of the Delphi session in Cyprus

Results (2)

The selected features of the BIRO Architectural structure can be summarized as follow:

- The selected BIRO architectural option has been identified in the **"Aggregation by group of patients"**, where grouping conditions are directly set by statistical object
- According to Delphi Results, the *sharing of personal information/data clusters* in the SEDIS information System should occur as follow:
  - Min. aggregation of N=5 patients per cell, only applicable for high critical privacy variables
  - Data aggregated at level of service centre
  - Aggregation of multidimensional patterns allowed (Min N=5 conditions)
- *The transmission of data to BIRO* requires the de-identification of data, where DATE fields have to be approximated to time interval (e.g. months) and a pseudonym should be used for service centre
- *The security mechanisms* for data transmission were identified in the adoption of a password access for local administrator prompting client program to send encrypted bundles to BIRO
- *The format of the BIRO database*, averaged over time, provides for separate sets of aggregated tables linkable by pre-defined statistical criteria
- Data shall be *disclosed* only to the BIRO database administrator and the *storage/retention site* has been indicated in the BIRO Coordinating Centre

Discussion

Legislative Review:

- Definition of privacy
- The 1948 Universal Declaration of Human Rights
- European Convention for the protection of Human Rights and Fundamental Freedoms (1950)
- Council of Europe's Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (1981)
- OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal data (1981)
- Charter of Fundamental Rights of the European Union (2000)
- European Constitution (2004)
- Additional Protocol to the Convention on Human Rights and Biomedicine concerning Biomedical Research (2005)
- The EU Data Protection Directive

Discussion (2)

The Privacy Legal Framework of the BIRO Project:

- Applicability of art. 8 (3) of the EU Data Protection Directive
- Recital 26 of the EU Data Protection Directive: Anonymisation
- Processing for statistical and research purposes (art 11, par. 2of the EU Directive
- Information to be given to the data subject: applicability of art. 10 and 11of the Directive
- Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data (1981): processing operations that poses no risk – applicability
- Tranborder data flow: 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.

Conclusions

- According to the privacy Impact Assessment of the BIRO Information System, the selected BIRO System Architecture, "**Aggregation by Group of Patients",** can be evaluated as the best privacy protective one, also considering the importance of the information content in terms of scientific soundness and the feasibility of the project in terms of technical complexity
- The BIRO System constructed is the best trade-off between privacy protection and the efficient and effective development and implementation of the system itself
- To be continued!