B.I.R.O.

WP5: PRIVACY IMPACT ASSESSMENT (PIA)

STEP 3:
“PRIVACY ANALYSIS REPORT”

ROMA MEETING
(20-21 OF APRIL 2008)

Concetta Tania Di Iorio
Serectrix snc
Tania_diiorio@virgilio.it

Structure of the Report

- Introduction
  - The BIRO project
  - The data model
- Scope of PIA Step 3: Privacy Analysis
- What has been achieved in previous PIA Steps
- Privacy Analysis
- Evaluation of privacy risks in the BIRO System
- Mitigation Strategies
- Conclusions

Scope of PIA Step 3: Privacy Analysis

- The privacy analysis examines the BIRO data flow in the context of applicable privacy policies and legislation
- The Data Flow Questionnaire, based on BIRO Data Flow Table, is the major source of information for the identification of any eventual privacy risks or vulnerabilities associated with the proposal

What has been achieved in PIA previous Steps

PIA main achievements, at present, have been:

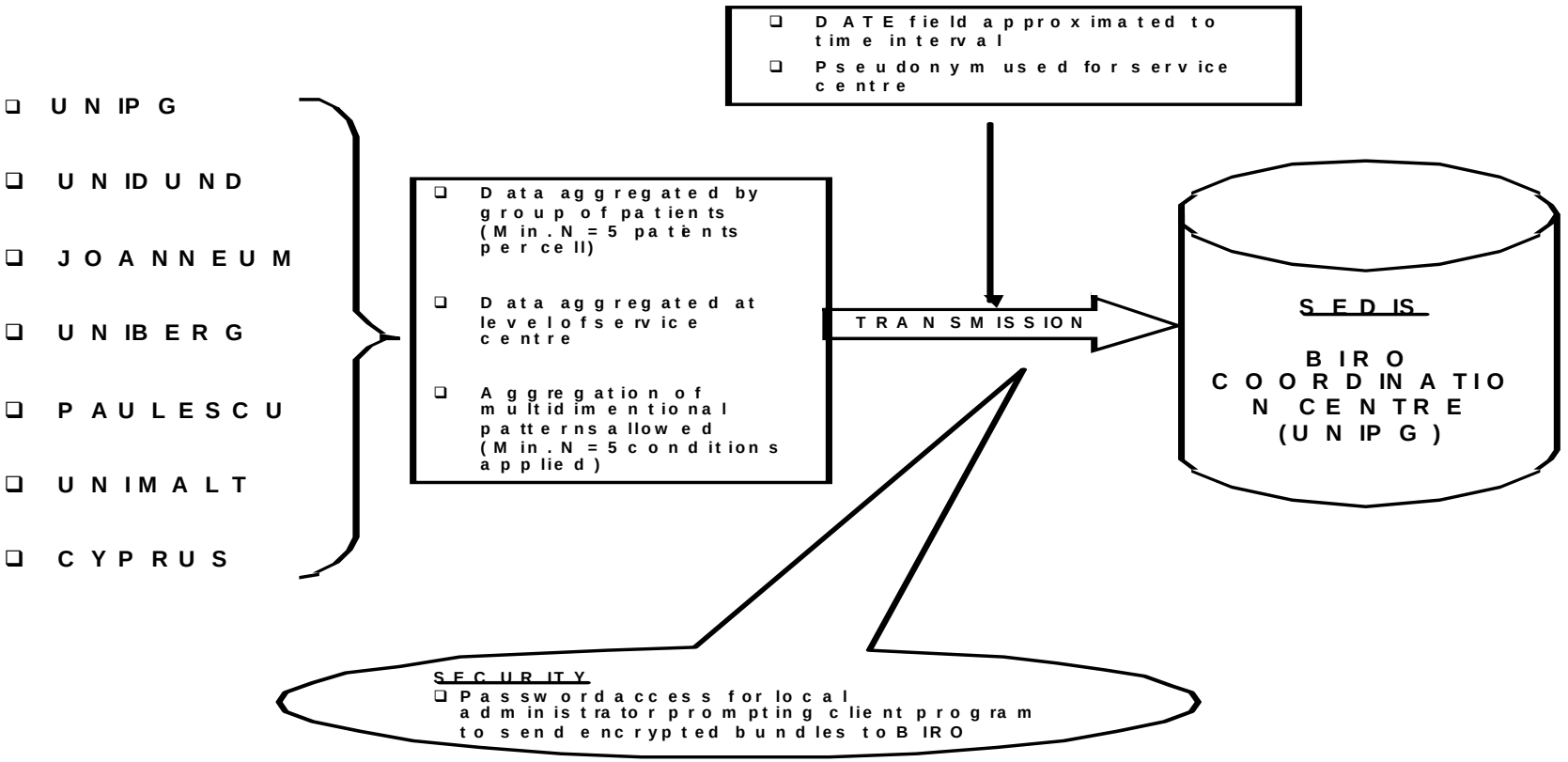
- The conduction of a legislative review, including a summary evaluation of potential privacy risks of the BIRO Information System
- The selection of three candidate alternatives for the SEDIS architecture:
  - Individual Patients Data, de-identified through a pseudonym
  - Aggregation by Group of Patients, centre IDs available, but de-identified
  - Aggregation by Region
- The data flow analysis:
  - describes and analyses the information flow occurring through the BIRO system in order to ultimately
- Identification of the best privacy protective BIRO architecture, according to the ongoing PIA

Privacy Analysis (1)

Source of information of the privacy analysis:

- The BIRO Diagram
- The BIRO Data Flow Table
- The Information Flow Questionnaire
- Overall Consensus Table,which summarises the questionnaire results (modified Delphi procedure)

B.I.R.O. Diagram



BIRO DATA FLOW TABLE- BIRO ARCHITECTURE: AGGREGATION BY GROUP OF PATIENTS

Description of personal information / Data clusters	*Collected by*	*Type of format*	*Used by*	*Purpose of collection*	*Transmission to BIRO: de-identification*	*Security mechanisms for data transmission*	*Format of BIRO Database*	*Disclosed to*	*Storage or retention site*
Aggregation by group of patients: min aggregation N=5, only applicable for high critical privacy variables e.g. service centre, geographical site etc	BIRO partner	One Record for each aggregation level	BIRO partner (local engine), BIRO Consortium (central engine)	Computation of single BIRO statistical object for local and SEDIS reporting	DATE fields approximated to time interval (e.g. months) Pseudonym used for service centre	. Password access for local administrator prompting client program to send encrypted bundles to BIRO	Separate sets of aggregated tables linkable by predefined statistical criteria	BIRO database administra-tor	BIRO Coordinating Centre
Data aggregated at the level of Service Centre									
Aggregation of Multidimensional patterns (e.g. risk adjustment) allowed with min N=5 condition applied									

Privacy Analysis (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. 2 of 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.

Evaluation of Privacy Risks & Mitigation Strategies

- Privacy risks identified after the privacy analysis of the BIRO information system are analysed through summary tables, which describe:
  - Element: individual data, aggregated data
  - Nature of risks: individual privacy
  - Level of risks
  - Comments: direct or indirect risk to privacy
  - Mitigating Mechanisms: reversible/non-reversible de-identification

- The level of risk is classified as follow:
  - 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.

Conclusions

At a general level, the kind of processing that take place in the BIRO centres should be 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: 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, unless domestic laws provides more stringent rules
- The norm constitutes an exemption to the prohibition of processing sensitive data, which is set forth by art. 8 of the Directive
- The exemption is justified by the need to protect the competing interests of society to a better health care

Conclusions (2)

- **Each centre of the BIRO consortium provides for the anonymisation of data before transferring them to the BIRO central database, where they are processed for statistical and scientific purposes**
- *According to Recital 26 of the Data Protection Directive,* **anonymisation** allows the processing of personal data without consent, placing anonymous data outside the scope of the data protection principles contained in the Directive. The processing of anonymous data is legitimate.
- 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

Conclusions (3)

Transborder data flow:

- The Centres involved in the BIRO project belong to European countries that have fully implemented the EU Data Protection Directive, and ratified the relevant Conventions
- 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.