2017

BRIDGE-Health Project Privacy and Ethics Evaluation

"Privacy and Ethics Impact & Performance Assessment" (PEIPA) Final Report

Dr. Concetta Tania Di Iorio
Legal Consultant LL.M M.P.H.
Serectrix snc
Email: ct.diiorio@serectrix.eu
On behalf of the University of Tor Vergata (UNITOV), Rome, Italy

(Grant Agreement n. 664691)

PRIVACY AND ETHICS EVALUATION

Privacy and Ethics Impact and Performance Assessment (PEIPA)

1. Background

The BRIDGE-Health project aims to create European health information (EU-HI) and data generation networks to support evidence-based health policy and research for the EU and Member States (MS), ultimately bridging to a future EU-HI research infrastructure consortium (ERIC-HI).

To this aim, the following objectives have been pursued:

- Enhance the transferability of health information and data for policy and improve the utility and use of data and indicators for stakeholders in policy making, public health surveillance and health care;
- Reduce health information inequality within the EU and within MS;
- Develop a blueprint for a sustainable and integrated EU Health information system by developing common methods for:
  - standardising the collection and exchange of health information within and between domains, between MS, including e-health platforms;
  - ensuring data quality, including procedures for internal and external validation of health indicators;
  - undertaking priority setting exercises for health information
  - addressing ethical and legal issues associated with the collection and use of health data within MS and the EU.

In order to address this latter objective, a collaborative and detailed work has been envisaged. Annex 1 of BRIDGE-Health Grant Agreement sets out the following work packages are involved in the ethical and privacy evaluation:

- <u>WP8 TASK 2</u>
  - Blueprints for adjusting and further developing a suite of open source software for data management, statistical analysis and automated delivery of indicators. The document will include a detailed plan of the development and implementation of a user friendly interface

    that will enable data custodians to produce local reports and transmit data towards a central location for the routine production of EU indicators (e.g. ECHI shortlist). The compliance of the whole process to privacy and data protection rules will be explored through the specification of targeted evaluation methods that will be made available to participating registers.

    - Development of technical manuals, including sets of recommendations for personnel involved in data processing of population-based registers

- WP10. Task 1
    - Support to Healthcare data systems in existing selected EU experiences. Meeting on ethical and legal issues; Expert advice on software development. Process: Analysis of ethical and legal issues from the countries; Output: Preliminary report on legal and ethical issues; Outcome/Impact: Ethical and legal aspects section included in the Technical Manual.
    - Deliverable: D10.2. Technical manual chapter on ethical and legal issues (Month 24);
- WP11: Privacy impact assessment: assessment of legal issues related to the approaches: contribution to the blueprint.

The accomplishment of the above tasks has been carried out through a **Privacy and Ethics Impact and Performance Assessment (PEIPA)**, a modified methodology of the Privacy Performance Assessment, developed and implemented in the EUBIROD project [(1-2).]

2. Privacy and Ethics Impact and Performance Assessment (PEIPA) Methodology

The PEIPA methodology consists of the following steps:

- Step 1: Identification and definition of key elements of ethics and privacy/data protection (Ethics and Privacy Factors)
- Step 2: Adoption of a Targeted Tool (PEIPA questionnaire) & nomination of the Advisory Panel of Experts
- Step 3: Analysis of ethics and privacy factors and variability of approaches at the European level
- Step 4: Final Report

Step 1. Identification and definition of key elements of ethics and privacy/data protection (Ethics and Privacy Factors)

The first step involves the description and analysis of EUBIROD, ECHO and EUROHOPE data sources and data flows and a review of privacy and ethics literature to identify privacy and ethical principles/norms involved in data processing operations occurring within registers/data sources to be analysed.

Reference documents to define the BRIDGE-Health project Ethics & Privacy Framework are as follows:

- EUBIROD Privacy Impact Assessment Report [(1)]
- OECD Health Information Infrastructure Report [(3)]
- OECD, Health Data Governance Report [(4)]
- Recommendation of the OECD Council on Health Data Governance [(5)]
- Regulation (EU) 2016/679, General Data Protection Regulation [(6)]

Step 2. Adoption of a Targeted Tool (PEIPA questionnaire) and Advisory Panel of Experts

The PEIPA Questionnaire is based on the model envisaged in the Privacy Impact Assessment Questionnaire developed in EUBIROD[(1)], but integrated with Ethics principles and findings from the Organisation for Economic Co-operation and Development (OECD) HCQI study[(3)], the OECD Advisory Panel of Health Information Infrastructure[(4)], the Recommendation of the OECD Council on Health Data Governance[(5)] and the new data Protection Regulation[(6)].

Scope of the PEIPA questionnaire is to acquire detailed information on how data is processed by involved participants: EUBIROD, ECHO and EUROHOPE consortia.

The PEIPA Questionnaire aims to:

- determine the level of privacy protection and ethical principle compliance of registries/databases/information systems involved in the above consortia

- evaluate how heterogeneous is the implementation of privacy-ethical principles/requirements among participating centres
- identify key areas of concern in the implementation of privacy-ethical principles/requirements across participating centres
- determine an optimal level of privacy and ethics (best practices) to be used as benchmarks for privacy/data protection and ethics clearance

An **ad hoc Advisory Panel of Experts** has been nominated for the revision of the “Privacy and Ethics Impact and Performance Assessment (PEIPA) Questionnaire”, along with the scoring system, in order to ensure that resulting benchmarks for privacy/data protection and ethics clearance are widely agreed upon, and based on objective and validated metrics.

Step 3. Analysis of ethics and privacy factors and variability of approaches at the European level

Results from the questionnaires have been analysed through a quali-quantitative methodology developed in the EUBIROD project (1, 2) and further tailored for the BRIDGE-Health privacy/data protection and ethics impact assessment. The PEIPA **scoring system** is developed by Serectrix, and reviewed and agreed upon by the hoc Advisory Panel of Experts.

Step 4. Final Report

A Privacy and Ethics in Person Meeting has been held in Cyprus, on 21st September 2017. The ad hoc Advisory Panel of Experts met to fine-tune the analyses of the ethical and privacy issues related to the information systems adopted by the EUBIROD, ECHO and EUROHOPE consortia, as highlighted by the PEIPA Questionnaires results. An open section was held to present the PEIPA methodology and results to the BRIDGE-Health participants.

The present final Report (Privacy & Ethics Impact and Performance Assessment Report) describes the ethical and privacy issues involved in the management of the above information systems and provides the results of the Privacy and Ethics Impact and Performance Assessment, along with the provision of objective benchmarks to identify best practices in the implementation of privacy and ethically compliant disease registries/information systems/databases.

3. STEP 1: EUBIROD, ECHO and EUROHOPE Data Flow & Identification and definition of key elements of ethics and privacy/data protection (Ethics and Privacy Factors)

The first step involves the description of EUBIROD, ECHO and EUROHOPE data sources and data flows and the identification of privacy and ethical principles/norms involved in data processing operations occurring within registers/data sources to be analysed. Reference documents to define the BRIDGE-Health project Ethics & Privacy Framework are as follows:

- EUBIROD Privacy Impact Assessment Report (1)
- OECD Health Information Infrastructure Report (3)
- OECD, Health Data Governance Report (4)
- Recommendation of the OECD Council on Health Data Governance (5)
- Regulation (EU) 2016/679, General Data Protection Regulation (6)

3.1. EUBIROD

The EUBIROD Network implemented the BIRO health information system, a "Shared Evidence-Based Diabetes Information System" (SEDIS), in 19 European countries.

The system has a structured architecture that involves two data processing steps, corresponding to a local and a global component, linked by a uni-directional flow of information (Figure 1).

A basic version of the system runs in each single register ("local SEDIS") to produce initial estimates for the local population. All partners in the network, using the same standardized procedures, repeat the process at their best convenience. Regional estimates are then sent to a central server that compiles "partial" results into a European report ("global SEDIS"). A web portal delivers user-friendly information for local registers.

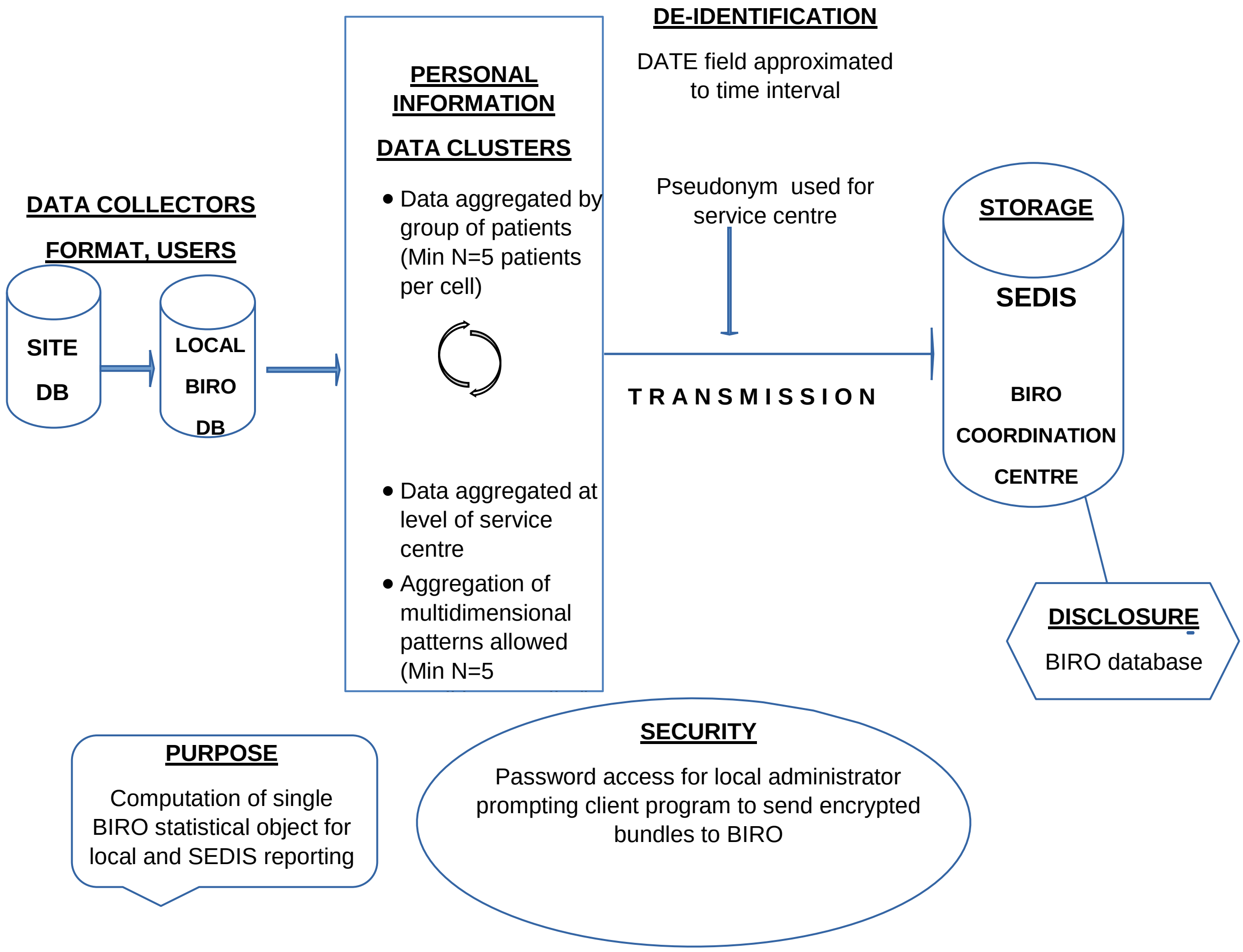
Functionality of the system is ensured by three fundamental elements: a concept and data dictionary including standardized evidence-based definitions in XML format; a report template to structure presentation of end results; and statistical methods required to produce them.

The same structure is used to automate the production of BIRO reports for individual centres and the whole network.

The data model includes a BIRO XML export, loaded by a Java-powered "Database Manager" into a local (Postgres) database that is directly accessed by R statistical routines to produce aggregate results. "Statistical objects" are defined as "elements of a distributed information system carrying essential data in the form of embedded, partially aggregated components that can be used to compute a summary measure or relevant parameter for the whole population from multiple sites".

Communication software is used to send statistical objects to a central server, where an ad hoc Java Importer loads them into a central BIRO database, and a global repository is maintained.

Figure 1: BIRO System Architecture


DE-IDENTIFICATION
DATE field approximated to time interval
Pseudonym used for service centre
PERSONAL INFORMATION
DATA CLUSTERS
• Data aggregated by group of patients (Min N=5 patients per cell)
• Data aggregated at level of service centre
• Aggregation of multidimensional patterns allowed (Min N=5
DATA COLLECTORS
FORMAT, USERS
SITE DB
LOCAL BIRO DB
TRANSMISSION
STORAGE
SEDIS
BIRO COORDINATION CENTRE
DISCLOSURE
BIRO database
SECURITY
Password access for local administrator prompting client program to send encrypted bundles to BIRO
PURPOSE
Computation of single BIRO statistical object for local and SEDIS reporting

Functions are used to process aggregate data submitted by local registers until a global pooled estimate is produced and published in pdf and html format on a dedicated web portal.

The BIRO system[(4)] involves medical records collected by diabetes registries at national or regional level, processed to support benchmarking and public health monitoring at the international level.

In terms of data transmission, BIRO centres send only aggregate records to the central server. For the most sensitive variables, aggregated records are not transmitted if groups contain less than five patients. Statistical objects are sent as tables stored in compressed bundles of flat text comma delimited files (CSV). Hence, there is no possibility, either directly or indirectly, that a patient could be identified with “reasonable means”.

The BIRO system[(7)] involves medical records collected by diabetes registries at national or regional level, processed to support benchmarking and public health monitoring at the international level.

Since the disclosure of information related to clinical centres or individual professionals could jeopardize the level of data sharing and eventually discourage participation to the project, EUBIROD Centres' IDs have been protected through the use of a pseudonym, together with a reporting system based on percentages rather than absolute numbers. Accordingly, the size of single Centres would be hidden, avoiding their indirect identification by third parties.

Aggregated statistical objects are sent to the central statistical engine to carry out global analysis.

Communication software has been specifically developed to ensure secure information exchange between the regional systems and the central SEDIS. To facilitate secure data transmission in BIRO, modern technologies have been selected and successfully used, complying with security requirements enshrined in both the EU and international data protection norms.

Global reporting does not pose any direct or indirect risk to privacy, as anonymous data sent by BIRO centres is transmitted to SEDIS in a secure environment and further processed in aggregate form.

With regard to trans-border data flow, although the central database is located outside national boundaries, the BIRO System processes only anonymous data; therefore, privacy and data protection rules are not applicable to this data processing. As a matter of fact, the processing of anonymous data falls outside the scope of the EU Data Protection Directive.

In accordance with EU and International legislation, reports will never allow either the data subjects or the local centres to be identified.

A privacy impact assessment of the BIRO system was conducted during the project lifetime and results were published on Journal of Medical Ethics(7)

A Privacy Performance Assessment was also conducted on EUBIROD centres, whose results were published on the European Journal of Public Health(2).

3. 2 ECHO(8)

The European Collaboration for Health Optimization (ECHO) is an international effort to gather healthcare information from several European countries within a single data warehouse (ECHO-DWH), specifically patient-level data from hospital admissions, demographic and socio-economic information at the geographic level, and supply information at both hospital and geographic levels. The countries participating in the project are Austria, Denmark, England, Portugal, Slovenia and Spain. Except Austria, all contributed data.

The goal of ECHO is to describe and analyse healthcare performance in terms of the utilization of effective (or lower-value) procedures, equity of access to effective care, and quality and efficiency (as determined by opportunity costs and technical efficiency). Unlike traditional international healthcare performance assessment, ECHO identifies unwarranted differences in performance within and across countries at different levels of analysis; hospital, healthcare area and region

ECHO is built upon routinely collected administrative data on hospital admissions, demographic and socio-economic characteristics of the population, hospital supply and geographic information.

Before any original dataset was released, ECHO team designed an information structure containing the basic data from each hospital episode that would allow building the ECHO performance indicators.[1] The information structure includes a set of variables that comprise the ECHO Core Table[2] and was used to integrate the original hospital administrative datasets into a single coherent relational database.

Some of these variables are patient attributes (e.g., age, sex, diagnoses and procedures), others are episode attributes (e.g., type of discharge or hospital of treatment), and others permit patient geo-allocation (mare_id). A KEY variable (ECHO_key) is also created automatically; this is a univocal numeric variable for each episode that allows coherent episode traceability and linkage across the different datasets and catalogues that comprise the ECHO-DWH. Finally, two other variables, mare_id and hospital_hist_id, allow linkage with additional datasets containing demographic, socioeconomic and supply information, thus allowing the allocation of this information at different geographic levels.

ECHO analyses the exposure to health services of (averages of the period) 5.4 million people in Denmark, 50.6 million in England, 10.1 million in Portugal, 2 million in Slovenia and 44.2 million in Spain. For all ECHO countries, ECHO-DWH contains a record of virtually all the hospitalizations recorded in ECHO countries for the reported years. The ECHO-DWH contains more than 191.1 million hospitalization episodes, corresponding to 841.6 million days of stay.

Socio-economic data is used to study factors that contribute to unwarranted variation in performance.

The ECHO-data warehouse

The ECHO-DWH has been designed as a relational database in which information from hospitalization episodes is linked to contextual information (namely, demographic statistics, socioeconomic data and information on supply) to produce intermediate and final outputs.

The data model is built upon three entities (episodes, hospitals and geographic areas) and their respective attributes. The critical attributes are described along various catalogues – dictionaries containing codes for diagnoses and procedures, hospital names and situations, name of each area in all geographic levels and population living in them.

A Critical element in the relational model is that episodes (dark-grey boxes) store individual patient-level information that is actually embedded into both a hospital and a geographic area. Consequently, linkage across files follows either a 1-to-1 scheme (when linkage is limited to episode-based attributes; dark to dark-grey arrows) or a 1-to-N scheme (when episodes are linked to a hospital or an area; dark to pale-grey arrows). To enable this linkage scheme, three key internal univocal key variables were constructed: echo_key (episode), hosp_hist_id (hospital) and mare_id (geographic area).

[1] ECHO performance indicators were actually an evolution of ARQH quality indicators (*http://*www.**qualityindicators.ahrq**.gov), the Health care quality indicators project by the OECD (http://www.oecd.org/els/health-systems/healthcarequalityindicators.htm) and, the Atlas VPM indicators project (www.atlasvpm.org).

[2] The 23 ECHO core variables are available at http://www.echo-health.eu/handbook/documents/ECHO%20INFORMATION%20SYSTEM%20REPORT%20FINAL.pdf

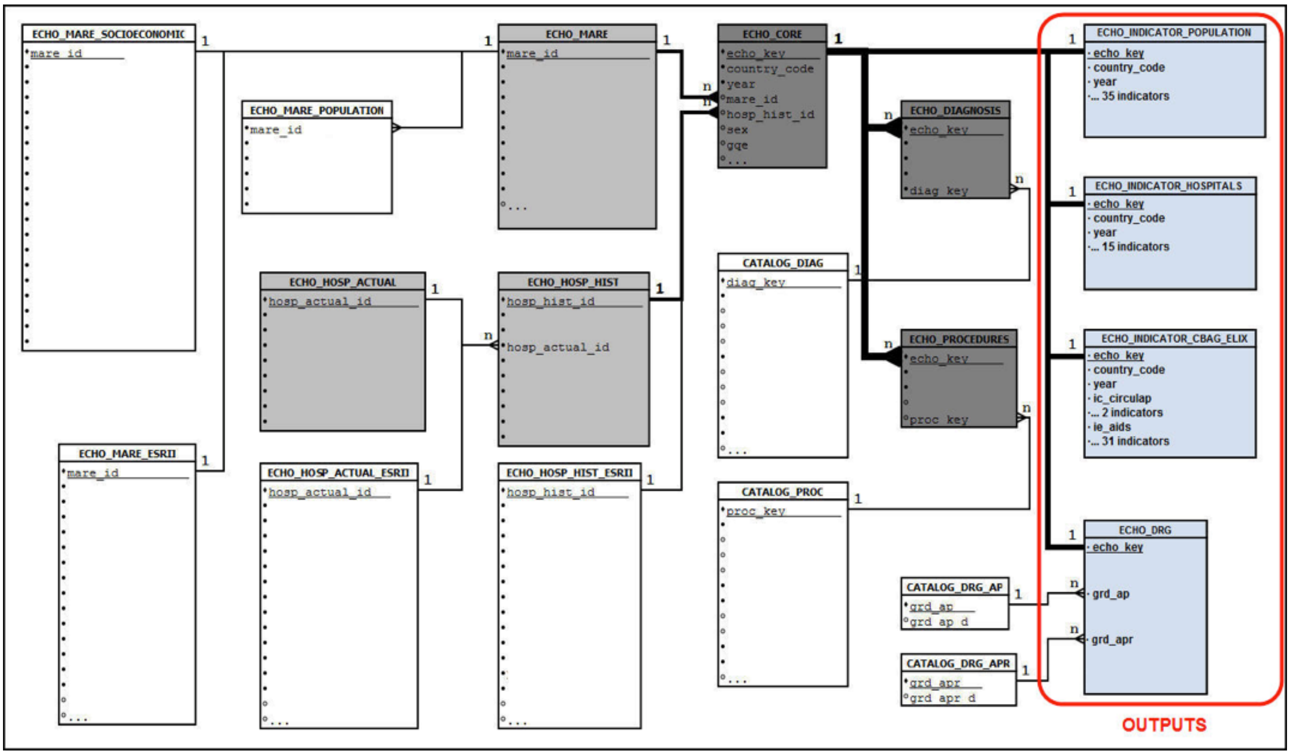


Figure 2: ECHO -DWH relational model scheme

3. 3 EUROHOPE[(9)]

The EuroHOPE (European Health Care Outcomes, Performance and Efficiency) project [(7)] aims to develop methods for performance assessment that can be used for routine evaluation.

The project uses linkable patient-level data available from national sources of Finland, Hungary, Italy, The Netherlands, Norway, Scotland and Sweden.

The project concentrates on five important disease groups: acute myocardial infarction (AMI), ischemic stroke, hip fracture, breast cancer and very low birth weight and preterm infants (VLBWI).

The EuroHOPE project developed an international comparative **database** that allows performance analysis, research and use indicators calculated at national, regional and hospital levels (Fig. 1). The disease-based approach requires patient-level data covering the whole population and the possibility to deterministically link records in different national registers. In the six countries (Finland, Hungary, the Netherlands, Norway, Sweden and Scotland) included in the EuroHOPE project it was possible to link national hospital-discharge registers with mortality registers and in five countries (excluding Scotland) also with registers of prescribed medicines. In Italy, similar data were available for two geographical areas. All databases present population data reflecting patterns of care and outcomes of the entire population residing in the defined territories.

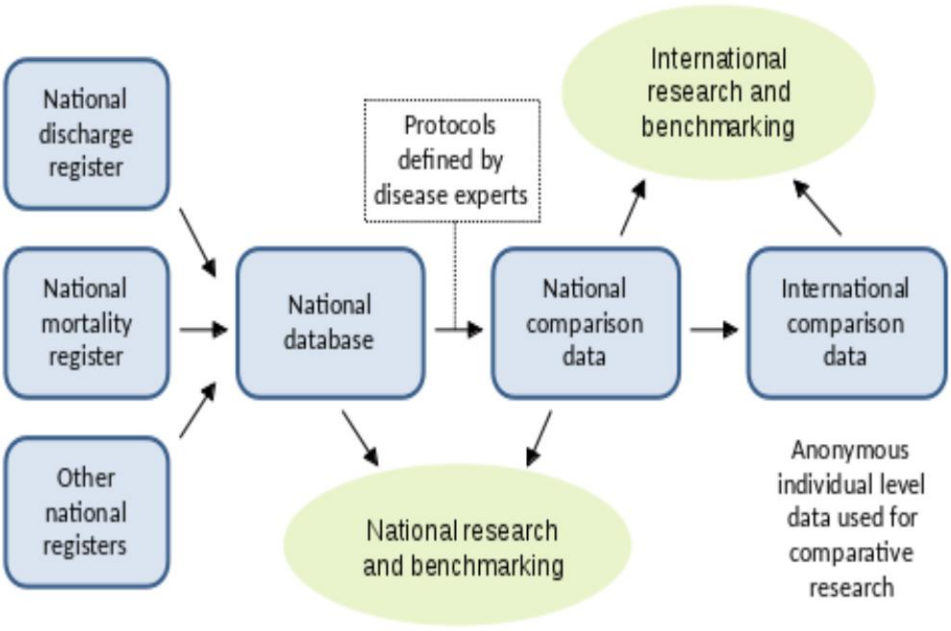
The main objective of the database is to produce performance indicators at country and regional and hospital level from the years 2006-2014 for international benchmarking. The database enables to extend and deepen the international comparative research on relationship between outcomes/quality and costs/resources as well as on the reasons behind the differences in outcomes and costs, (Hagen et al. 2015, Häkkinen et.al 2015).

This specific protocol for international comparisons for AMI is based on the data of hospital discharge registers, mortality registers, and other available administrative health care registers (such as medication use, specialty visits, etc.). The protocol is used for preparing both the **national acute coronary syndrome (ACS) databases for each country and for an international comparative (ACS) database,** which was produced using the national stroke databases.

Construction of data

Every country has established a **national AMI and ACS database**. Using personal identification number patients' information is linked to the following registers:

- Hospital discharge registers
- Outpatient services in specialist care / hospitals
- Data from other institutions (e.g. nursing homes)
- Drug utilisation registers
- National mortality registers
- Primary health services and care of the elderly (Metropolitan study)


National discharge register
National mortality register
Other national registers
National database
Protocols defined by disease experts
National comparison data
International comparison data
International research and benchmarking
National research and benchmarking
Anonymous individual level data used for comparative research

3. 4. Privacy & Ethics Principles

The key elements of privacy/data protection and ethics (factors) identified as relevant in the Privacy and Ethics evaluation of the BRIDGE-Health project consortia are as follows:

1. *Responsibility for Personal Data*, which focuses on privacy policies and measures implemented by data controllers;
2. *Collection and Use of Personal Data*, relative to the legal base to collect personal data, the necessity of the information collected (minimality principle), the use of information for secondary purposes, the provision of anonymization for planning, management and/or evaluation purposes;
3. *Consent*, on the necessity to gather informed consent for the collection and processing of data in the registry/database/information system and on how consent is obtained, if it is informed and unambiguous, if broad consent is allowed;
4. *Data Sharing*, focusing on the possibility for data controllers to share data for specified purposes (e.g. governmental, research, commercial purposes);
5. *Data Linkage*, focusing on means and techniques used for data linkage;
6. *Access and Accuracy of Personal Data*, dealing with the possibility for individuals to access, object, request the rectification of personal data;
7. *Safeguarding Personal Data*, related to security measures and processes;
8. *Anonymisation Process,* which analyse the whole compliance with international technical standards and principles
9. *Openness*, Transparency and Public Engagement, with regard to communication processes and strategies with the public
10. *Transparent Project Approval Processes*, on the mechanisms implemented in project approval process
11. *Beneficence/Non Maleficence in Health Research Project Approval Processes*, on the application of ethics principles in project approval processes.

4. STEP 2: Adoption of a Targeted Tool (PEIPA questionnaire) & Nomination of the Advisory Panel of Experts

4.1 Nomination of Advisory Panel of Experts

An ad hoc Advisory Panel of Experts has been nominated for the revision of the "Privacy and Ethics Impact and Performance Assessment (PEIPA) Questionnaire" to ensure that resulting benchmarks for privacy/data protection and ethics clearance are widely agreed upon and based on objective measurements. The ad hoc Advisory Panel of Experts is composed of the following Members:

Surname	**Name**	**Institution**	**Country**
Smith	David	Former Deputy UK Information Commissioner	UK
Hamalainen	Paivi	National Institute of Health and Welfare (THL)	Finland
Siano	Manuela	Data Protection Authority	Italy
De Marco	Dorotea	Data Protection Authority	Italy
Oderkirk	Jillian	OECD Health Division	France
de Lusignan	Simon	University of Surrey	UK

4.2 The PEIPA Questionnaire (Appendix 1)

The questionnaire is a core element of the PEIPA, providing input for the privacy and ethics analysis**.** The instrument draws upon the EUBIROD Privacy Impact Assessment(1,2), the OECD Health Information Infrastructure Study(3), the OECD Eight Data Governance Mechanisms that maximise societal benefits and minimise risks(4), the Recommendation of the OECD Council on Health Data Governance(5) and Regulation (EU) 2016/679, General Data Protection Regulation(6).

The questionnaire is specifically addressed to data controllers and/or data protection officers and/or chief executive officers responsible for data processing occurring in the registries/databases/information systems of the BRIDGE-Health consortia; namely: ECHO, EUROHOPE and EUBIROD.

The questionnaire has been administered by Serectrix snc on behalf of the University of Tor Vergata (Italy), in collaboration with Consortia Coordinators, who facilitated submission and collection of the questionnaires to and from participating centres.

The questionnaire is composed of 11 sections (factors), each containing a specific number of questions (sub-factors).

The key elements of privacy/data protection and ethics (factors) identified in step 1 of the PEIPA process as relevant in the Privacy and Ethics evaluation of the BRIDGE-Health project are as follows:

1. *Responsibility for Personal Data*, focusing on privacy policies and measures implemented by data controllers to ensure accountability;
2. *Collection and Use of Personal Data*, relative to the legal base to collect personal data, the necessity of the information collected (minimality principle), the use of information for secondary purposes, the provision of anonymization for planning, management and/or evaluation purposes;
3. *Consent*, on the necessity to gather informed consent for the collection and processing of data in the registry/database/information system and on how consent is obtained, if data controllers are able to demonstrate that consent has been freely given, informed and unambiguous, if broad consent is allowed;
4. *Data Sharing*, focusing on the possibility for data controllers to share data for specified purposes (e.g. governmental, research, commercial purposes);
5. *Data Linkage*, focusing on means and techniques used for data linkage;
6. *Access and Accuracy of Personal Data*, dealing with the possibility for individuals to access, object, request the rectification of personal data;
7. *Safeguarding Personal Data*, related to security measures and processes;
8. *Anonymisation Process,* which analyse compliance of the sample with international technical standards and principles
9. *Openness*, Transparency and Public Engagement, with regard to communication processes and strategies to inform and engage the public
10. *Transparent Project Approval Processes*, focusing on the mechanisms implemented in project approval processes
11. *Beneficence/Non Maleficence in Health Research Project Approval Processes*, on the application of ethics principles in project approval processes.

Results from questionnaires have been analysed through a mixed quali-quantitative analysis. Results will be made available to participants and to the wider community in de-identified and/or aggregated format, also via the present Final Report. Respondents IDs will not be revealed, except to each participant concerned.

The PEIPA methodology is not aimed to rank systems or to produce league tables, but to enhance quality improvements mechanisms in the management of health information.

4.3 PEIPA Questionnaire Scoring System (Appendix 2)

Sections in the PEIPA questionnaire refer to specific "privacy factors" (e.g. Section 1: responsibility for personal data) that have been identified in relation to specific EU and/or international data protection and ethics principles or norms.

Factors provide summary results that are easy to interpret for all questions included in the questionnaire. Each section is composed of questions that can be seen as "sub-factors (e.g. Question 1.1: Has the data controller of the registry/database/information system been nominated"?), drilling down into specific procedures that are relevant to fulfil privacy and ethics goals.

Standardized coding has been applied to deliver a quali-quantitative analysis for all questions and factors included in the questionnaire.

The scoring system aims to ascertain the adherence to privacy and ethics principles or norms of selected processing operation undertaken by members of ECHO, EUROHOPE and EUBIROD consortia.

The original responses (YES-NO-N/A) have been coded by assigning:

- A mark of 1 to any privacy protective and ethically compliant conduct regardless of a YES-NO-N/A response. Weighed marks have been also assigned whether necessary, as specified in the scoring tables (see appendix 2)
- A mark of zero to any privacy and ethically not-protective/compliant practice
- N/A responses to single questions are assigned either a mark of 0 (most cases) or 1, according to scoring tables (see appendix 2)
- Missing and N/A responses relative to entire sections have been excluded by the calculation of mean, median and total scores of the sample.

The scoring system has been revised and agreed by the Advisory Panel of Experts.

Factors are computed as the linear sum of recoded values (of the original responses).

Scaled factors are computed as a percentage of each factor score on the total attainable score.

The overall level of privacy and ethics protection has been computed as the average of all scaled factors for each participating centre.

5. STEP 3: Results & Analysis of ethics and privacy factors

5.1 Results

The eleven sections contained in the PEIPA questionnaire describe a broad range of elements related to the respect of privacy and data protection legislation, the adherence to some ethical principles in the conduct of research projects, and the implementation of internationally recognized best practices (e.g. OECD guidelines and best practices). These elements should be duly taken into account in the management of registries/databases/information systems processing health and health related data.

Hence, results from the questionnaire describe the level of legal compliance and adherence to ethical principles and best practices achieved by study participants.

The "results" section is divided into five sub-sections:

1. Main findings from single questions: overall percentage of YES-NO-N/A responses registered by the whole sample for each of the selected questions;

2. Factors: scaled scores achieved by the whole sample in each privacy and ethics factor. This sub-section provides an evaluation of the adherence to privacy/data protection and ethics principles of responding centres in any factor identified;

3. Overall privacy performance evaluation: overall level of privacy/data protection and ethics achieved by the whole sample;

4. Privacy/Data protection and Ethics Performance by Consortia;

5. Privacy/Data protection and Ethics Profile of Participating Centre

5.1.1 Main Findings from single Questions

This sub-section of the report focuses on the results obtained by participating centres on selected questions that have been considered of particular interest for the study, providing a detailed description of how health and health related data are handled in the BRIDGE-Health sample of centres.

The following factors are presented in details:

1. Responsibility for Personal data
2. Collection and Use of Personal Data
3. Consent
4. Data Sharing
5. Data Linkage
6. Safeguarding Personal Data
7. Anonymisation Process

Factor 1: Responsibility for Personal data

This section investigates on the activities performed by data controllers to ensure accountability. Data controller is herein intended as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by Union or Member State law, the data controller or the specific criteria for its nomination may be provided for by Union or Member State law.

The selected questions for this factor are as follows:

- Q1.1: Has the data controller of the registry/database/information system been nominated?
- Q1.5: Has the data controller determined the set of purposes and means of the various processing3 occurring in the registry/database/information system?
- Q1.7: Has the data controller implemented appropriate technical and organisational measures embedding privacy protective technologies (e. g. pseudonymisation, encryption) in the registry/database/information system (privacy by design)?
- Q1.8: Has the data controller implemented appropriate technical and organisational measures to ensure, by default, adherence to privacy principles (e.g. data minimization principle) in the registry/database/information system?
- Q1.9: Does the data controller conduct privacy/data protection impact assessments, when processing involve a high risk for privacy; e.g. processing on a large scale of health related data?
- Q1.10: Has the data controller put in place measures to ensure that it is able to demonstrate and document the effectiveness of the above mechanisms (accountability)?

Results show that data controllers of the registry/database/information system are nominated in the 100% of the sample (N=15 centres).

The set of purposes and means of the various processing are determined by data controllers in the 73.4 % of cases; while are not determined in 13.3% of cases.

Data controllers implement appropriate technical and organisational measures to ensure, by default, adherence to privacy principles (e.g. data minimization principle) and appropriate technical and organisational measures embedding privacy protective technologies (e. g. pseudonymisation, encryption) in 93.4% of cases.

Data controllers conduct privacy/data protection impact assessments, when processing involve a high risk for privacy (e.g. processing on a large scale of health related data) in the 73.4% of cases.

However, data controllers put in place measures to ensure that they are able to demonstrate and document the effectiveness of the above mechanisms (accountability) only in the 66.7% of cases; i.e. data controllers were found unable to document accountability in the 26.7% of cases.

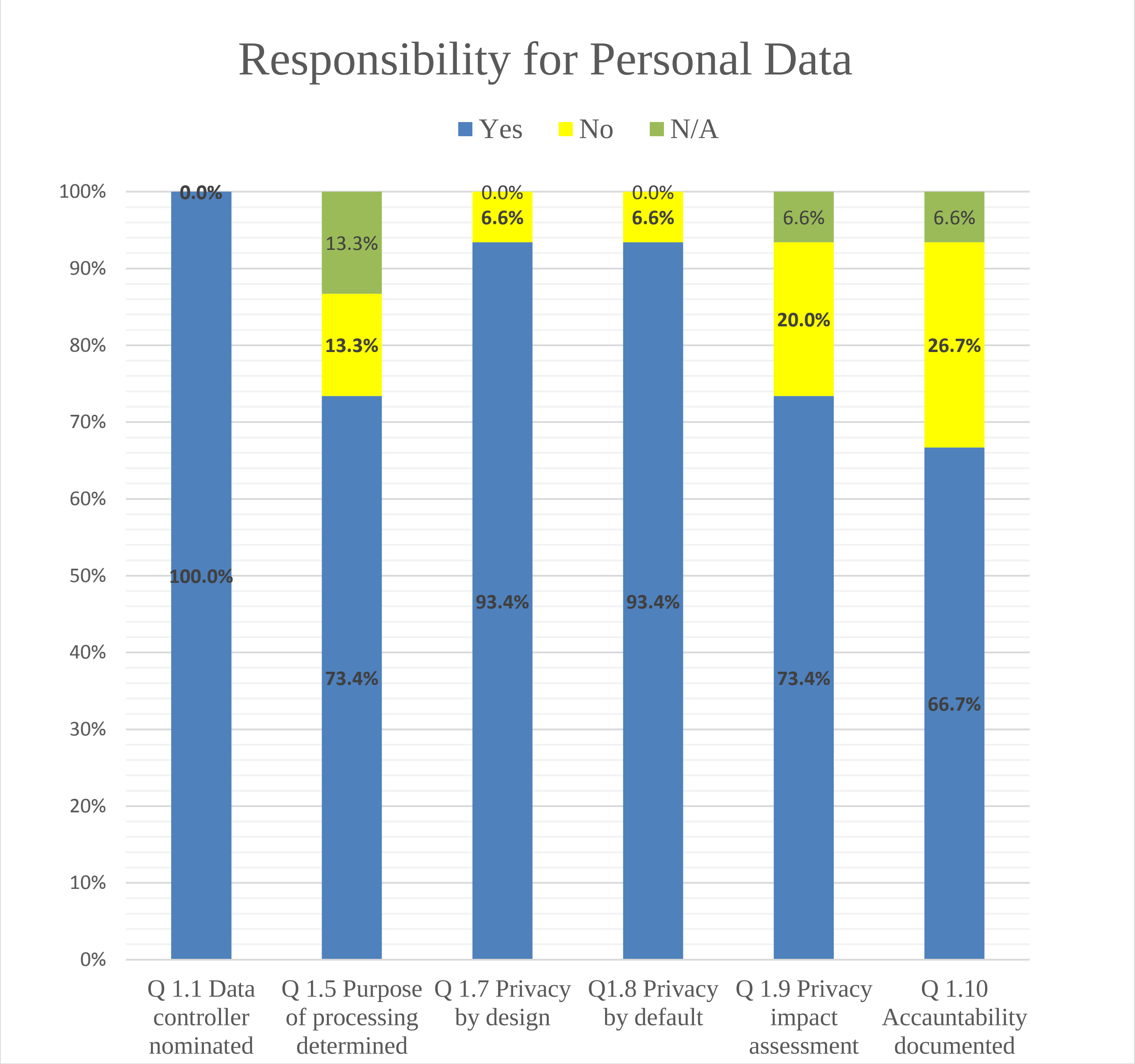


Figure1: Responsibility for personal data

Factor 2: Collection & Use of Personal Data

This section focuses on the means of personal data processing.

Personal data is intended as any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

The selected questions for this factor are as follows:

- Q 2.2: Do you collect personal data in the registry/database/information system with the data subject consent?
- Q 2.3: Is all the personal data collected necessary to the registry/database/information system; i.e. limited to what is necessary in relation to purposes of the registry/database/information system, as set out by the data controller?
- Q 2.4: Are data controllers of the registry/database/information system allowed to use data for secondary purposes1; e.g. approved health research and statistics?
- Q 2.5: If yes, are the secondary uses compatible with the purposes for which data were previously collected?
- Q 2.6: Is this data used to regularly report on health care quality or health system performance?
- Q 2.9: Is data de-identified and/or pseudonymised before it is used for any secondary purpose, including data linkage?

Responses to this factor highlight that only the 46.7% of the involved centres collect personal data with the data subject consent, the 46.7% does not collect personal data with the patient consent and 6.6% of the sample responded that the question was not applicable in their case.

The 86.7 % of the sample confirmed that personal data collected are necessary to the registry/database/information system; i.e. limited to what is necessary in relation to purposes of the registry/database/information system, as set out by the data controller; while in the 13.3% of cases the question was not applicable.

The 93.4% of data controllers stated they are allowed to use data for secondary purposes; e.g. approved health research and statistics. The 6.6% of the sample (N=1 centre) could not use data for secondary purposes. In the same cases, the secondary uses were compatible with the purposes for which data were previously collected.

Data resulted to be used to regularly report on health care quality or health system performance in 66.7% of cases and not used for this purpose in the 33.3% of cases.

The 100% of the sample reported that data were de-identified and/or pseudonymised before it is used for any secondary purpose, including data linkage.

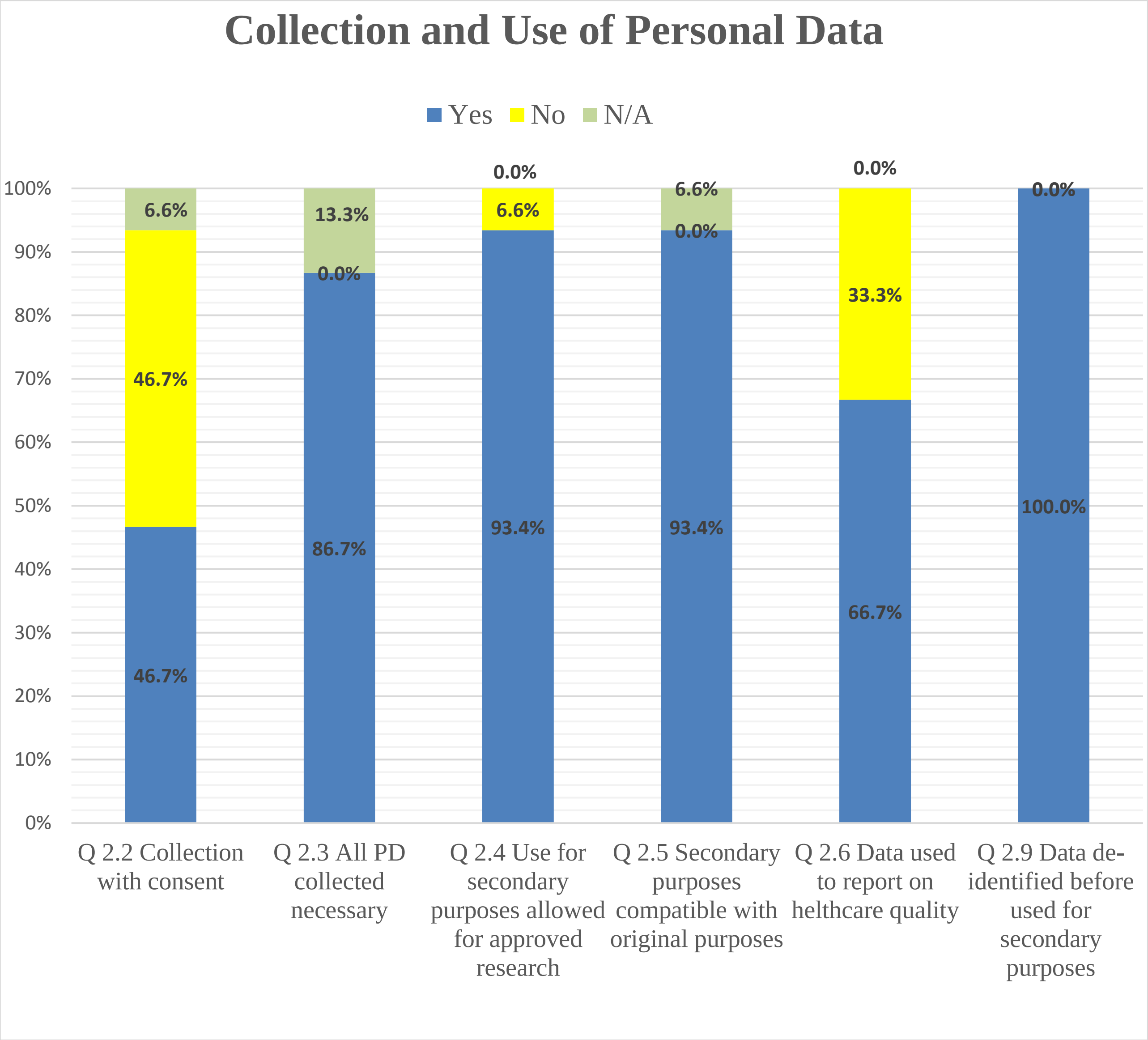


Figure 2: Collection and use of personal data

Factor 3: Consent

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

The selected questions for this factor are as follows:

- Q 3.1: Is consent required to collect and process personal health data in the registry/database/information system?
- Q 3.2: If consent is not required, is it waived by law?
- Q 3.3: If consent is not required, can the data subject opt-out?
- Q 3.4: If consent is required, is it obtained directly from the individual?
- Q 3.7 Can the data subject refuse to consent to the collection or use of personal information for a secondary purpose, unless required by law?
- Q 3.8: Can the data subject withdraw his/her consent at any time?
- Q 3.9: Is a broad consent to further uses of registry/database/information system data and/or data linkage allowed for approved health studies and research?
- Q 3.10: Is a broad consent to any further (non-health related research) uses of health data and/or data linkage allowed?

Results show that consent to collect and process personal health data in the registry/database/information system involved is required by 40% of the centres, while is not required in the 60% of cases (16.6%).

Where consent is necessary (40% of cases), it is obtained directly from the individual in the 83.4% of cases where consent is required; and not directly from the individual in the remaining cases.

Data subjects can refuse to consent to the use of their personal data for secondary purposes and can withdraw consent in the 66.8% of cases where consent is required.

A broad consent for approved health studies and research is allowed in the 66.8% of the sample of consent required cases; while a broad consent for any secondary purposes is not allowed in the 83.4% of cases.

When consent is not required (60% of cases), it is waived by law/regulation in the 100% of cases. However, only in the 11.1% of cases where consent is not required the data subject can opt out.

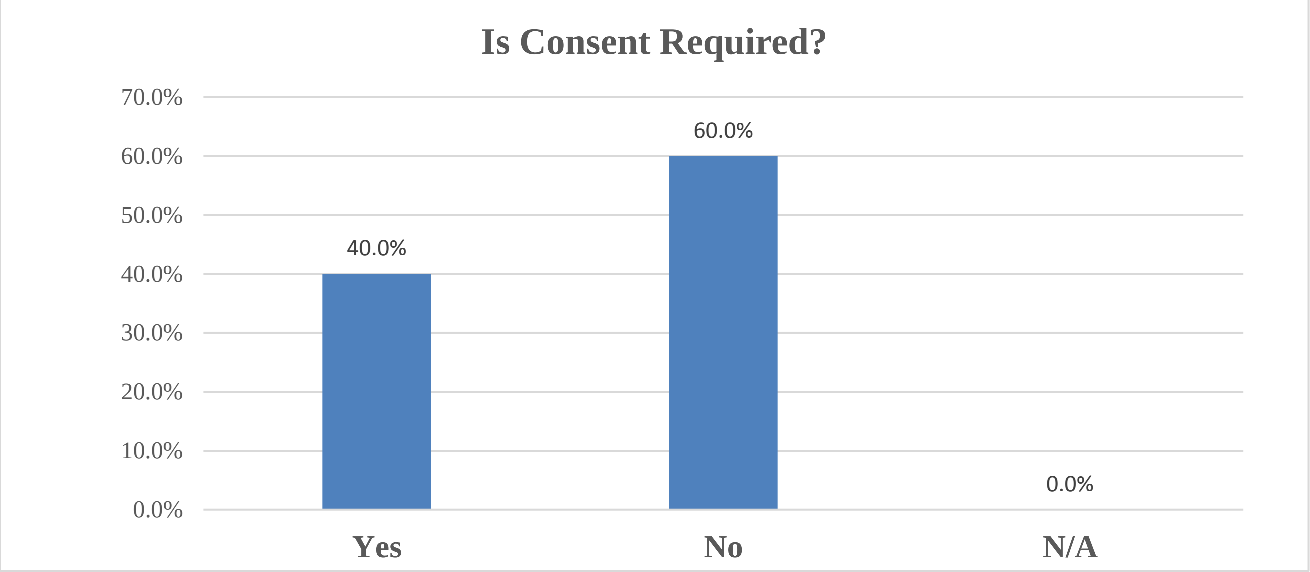


Figure 3: Consent required/not required

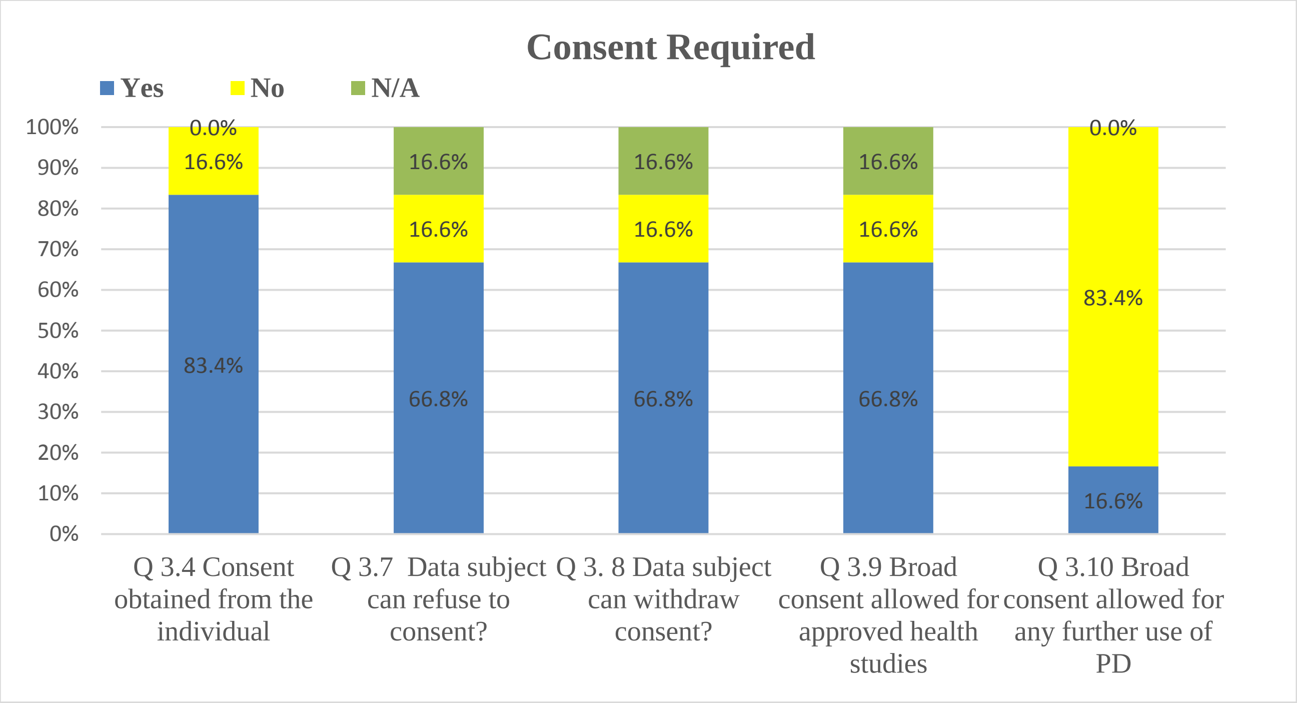
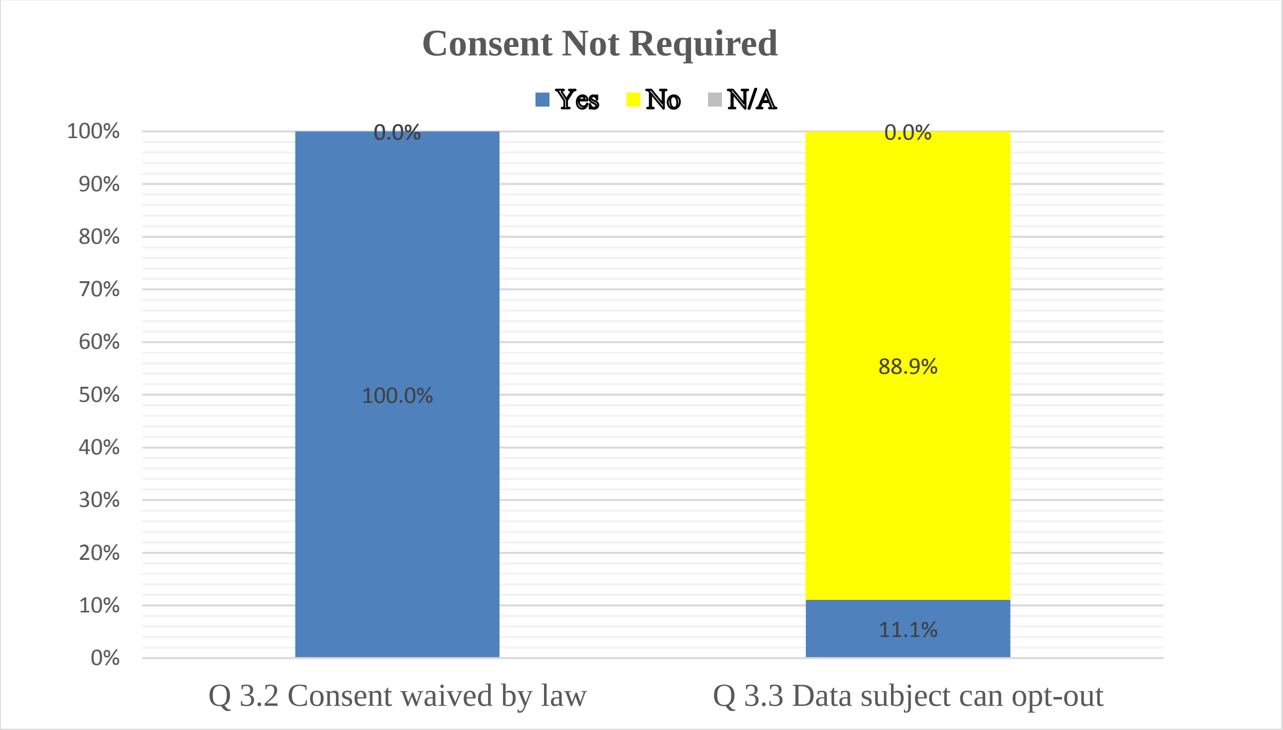


Figure 4: Consent required


Consent Not Required
Yes
No
N/A
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
0.0%
100.0%
0.0%
88.9%
11.1%
Q 3.2 Consent waived by law
Q 3.3 Data subject can opt-out

Factor 4. Data Sharing

Data sharing is intended as the transfer of data from one or more organisations to a third party organisation or organisations (recipient/recipients). Transborder data flow is a transfer of personal data to a recipient who or which is subject to a foreign jurisdiction. Article 2 (1) of the Additional Protocol to Convention 108 describes transborder data flow as the transfer of personal data to a recipient who or which is subject to a foreign jurisdiction. According to the EU General Data Protection Regulation (2016), cross-border processing means either:

- processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a data controller or processor in the Union where the data controller or processor is established in more than one Member State; or
- processing of personal data which takes place in the context of the activities of a single establishment of a data controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

The selected questions for this factor are as follows:

- Q 4.1: Are data controllers allowed to share readily identifiable health data for statistics or research with public authorities and/or academic or private organisations for non-commercial purposes?
- Q 4.2: Are data controllers allowed to share de-identified or pseudonymised health data with another public authority and/or academic or private organisations for non-commercial purposes?
- Q 4.4: Are data controllers allowed to share de-identified or pseudonymised health data for statistics and research with another foreign public authority and or academic or private organisations for non-commercial purposes?
- Q 4.5: Do you have a standard data sharing agreement for disclosing data (or multiple standard ones for different types of data requestors)?

According to EU privacy and data protection principles, the 86.7% of data controllers (N=13 centres out of 15) involved in the PEIPA are not allowed to share readily identifiable health data for statistics or research with public authorities and/or academic or private organisations for non-commercial purposes.

However, data controllers are allowed to share de-identified or pseudonymised health data with another public authority and/or academic or private organisations for non-commercial purposes in the 80% of cases; while the66.7% of the sample can share the same data also with another foreign public authority and or academic or private organisations for non-commercial purposes.

The 53.4% of the involved centres have a standard data sharing agreement for disclosing data or multiple standard ones for different types of data requestors.

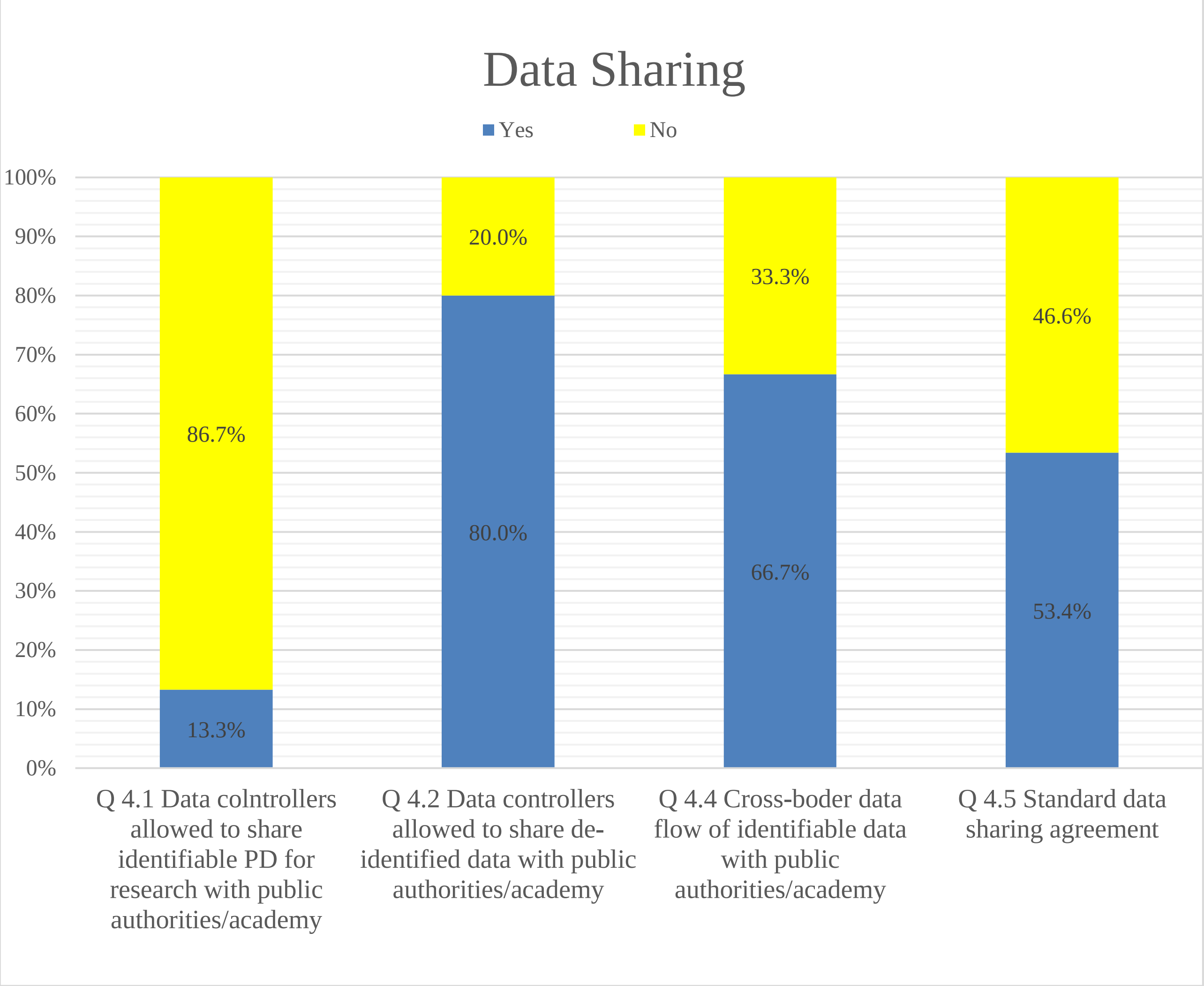


Figure 4: Data Sharing

Factor 5: Data Linkage

Record linkage refers to a merging that brings together identifiable records from two or more sources of data with the object of consolidating facts concerning an individual or an event that are not available in any separate record (Handbook of Vital Statistics Systems and Methods, Vol. 1: Legal, Organizational and Technical Aspects, United Nations Studies in Methods, Glossary, Series F, No. 35, United Nations, New York, 1991.) An example would be linking patient records in a hospital database to any death records for the same persons in a mortality registry in order to identify patients who died following treatment.

Deterministic record linkage, often referred to as exact matching, occurs when a unique identifier or set of identifiers is used to merge two or more sources of data. In health linkages, the identifier used is often a unique patient identifying number or UPI.

Probabilistic record linkage occurs when a set of possible matches among the data sources to be linked are identified. For example, identifying information such as names, dates of birth, and postal codes, may be used to assess potential matches. Then statistics are calculated to assign weights describing the likelihood the records match. A combined score represents the probability that the records refer to the same entity. Often there is one threshold above which a pair is considered a match, and another threshold below which it is considered not to be a match. This technique is used when an exact match between records across databases is not possible, or when data capture errors have caused deterministic matches to fail.

Sometimes deterministic matching does not provide a perfect match (e.g. matching on a unique local system ID which might be repeated on other local systems). In these circumstances mixed probabilistic and deterministic methods can be used (de Lusignan S, Navarro R, Chan T, Parry G, Dent-Brown K, Kendrick T. Detecting referral and selection bias by the anonymous linkage of practice, hospital and clinic data using Secure and Private Record Linkage (SAPREL): case study from the evaluation of the Improved Access to Psychological Therapy (IAPT) service. BMC Med Inform Decis Mak. 2011 Oct 13;11:61. doi: 10.1186/1472-6947-11-61).

The selected questions for this factor are as follows:

- Q 5.2: Is record linkage performed using the registry/database/information system records?
- Q 5.5: Do you apply standard practices for deleting direct identifiers (such as names and patient numbers) for the performance of data linkages?
- Q 5.6: Do you apply standard practices for deleting direct identifiers (such as names and patient numbers) after the data linkage has been finalized?
- Q 5.8: Is the de-identification and/or pseudonymisation methodology documented?
- Q 5.9: Do you use a standard process for the assessment of the risk of data re-identification?
- Q 5.10: Do you use standard practices for the treatment of attributes that pose a re-identification risk (such as rare diseases, exact dates, locations, or ethnic origins)?

Results show that the 80% of the involved centres performs data linkage (N=12 centres) using the registry/database/information system records. The 83.4% of centres that perform data linkage applies standard practices for deleting direct identifiers (such as names and patient numbers) for the performance of data linkages; while the 75% of centres applies these practices also after the data linkage has been finalized.

In 66.6% of cases the de-identification and/or pseudonymisation methodology is documented. However, the use of a standard process for the assessment of the risk of data re-identification is applied in only the 41.6% of the sample.

The 58.3% of centres uses standard practices for the treatment of attributes that pose a re-identification risks (such as rare diseases, exact dates, locations, or ethnic origins).

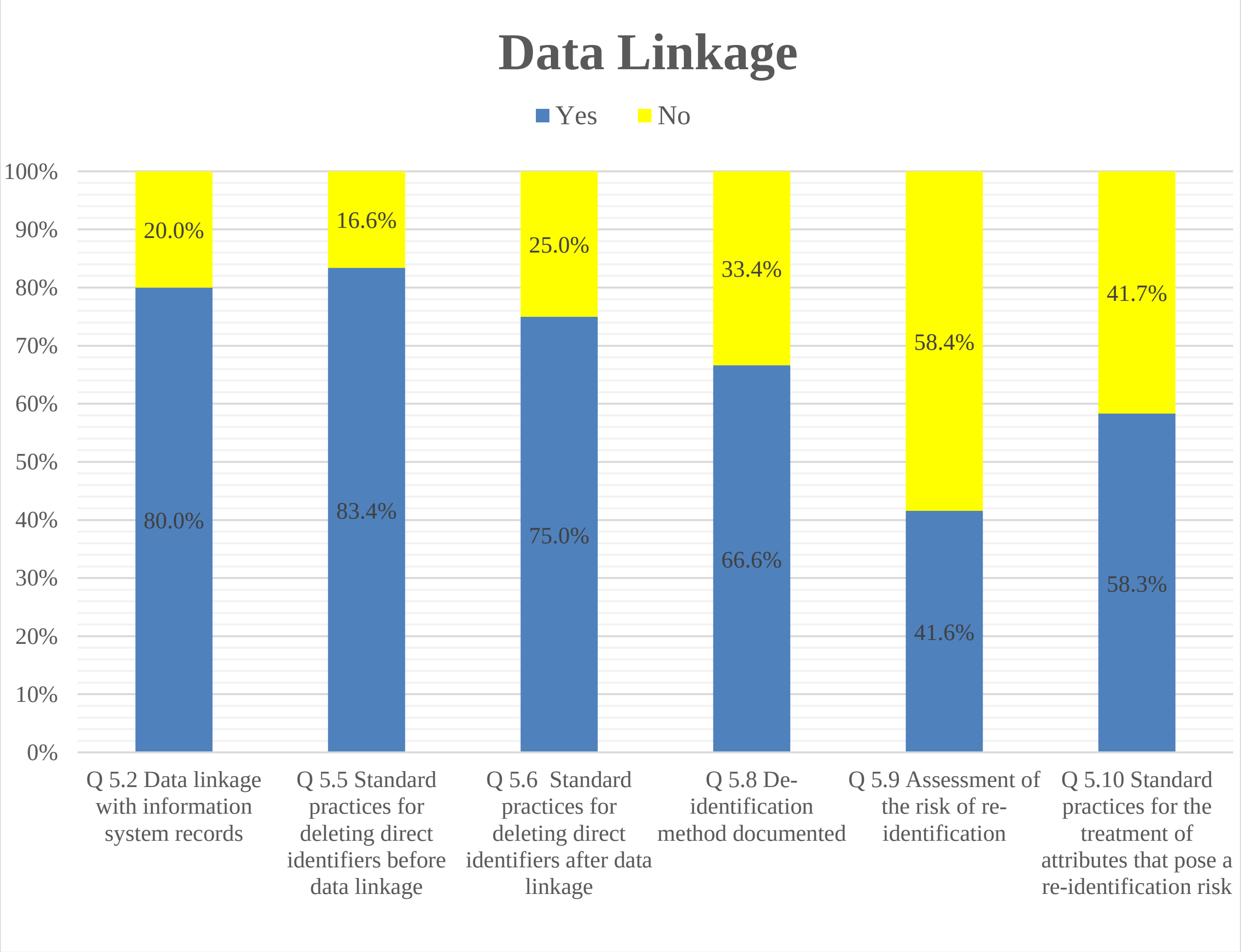


Figure 5: Data Linkage

Factor 7: Safeguarding Personal data

According to Art 32(1) of the General data protection Regulation (2016), the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- the pseudonymisation and encryption of personal data
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The selected questions for this factor are as follows:

- Q 7.1: Are security measures compliant with international standard according to the state of the art? E.g. Any of the following ones: ISO 27001:2013, a standard for information security management; ISO 27002:2013, a catalogue of information security controls; ISO 27005:2011, a standard for information security risk management?
- Q 7.2: Is compliance with international standards certified by accredited registration bodies (e.g. assessment and registration bodies, certification/ registration bodies or registrars)?
- Q 7.3: Have security procedures for the collection, transmission, storage and disposal of personal information, and access to it, been documented?
- Q 7.5: Are user accounts, access rights and security authorizations controlled by a system or record management process?
- Q 7.8: Are there contingency plans and documented procedures in place to identify and respond to security breaches or disclosures of personal information in error?
- Q 7.9: Are there documented procedures in place to communicate/notify security violations to the data subject, law enforcement authorities and relevant program managers when there is a risk to the rights and freedom of data subjects?
- Q 7.10: Is there a plan for quality assurance and audit programs to assess the ongoing state of the safeguards applicable to the system?

Results highlight that security measures are compliant with international standard according to the state of the art (e.g. ISO 27001:2013, standard for information security management; ISO 27002:2013, catalogue of information security controls; ISO 27005:2011, standard for information security risk management) in the 60% of the involved centres.

However, compliance with international standards is certified by accredited bodies (e.g. assessment and registration bodies, certification/ registration bodies or registrars) only in the 40% of cases.

Security procedures for the collection, transmission, storage and disposal of personal information, and access to it, are documented in 80% of cases.

In the 93.4 % of the centres user accounts, access rights and security authorizations are controlled by a system or record management process and employees are trained in the requirements for protecting personal information and are aware of the relevant policies regarding breaches of security, integrity or confidentiality.

Contingency plans and documented procedures are in place to identify and respond to security breaches or disclosures of personal information in error in the 53.4% of cases.

Documented procedures are in place to communicate/notify security violations to the data subject, law enforcement authorities and relevant program managers in the 53.4% of cases.

In the same cases there is a plan for quality assurance and audit programs to assess the ongoing state of the safeguards applicable to the system.

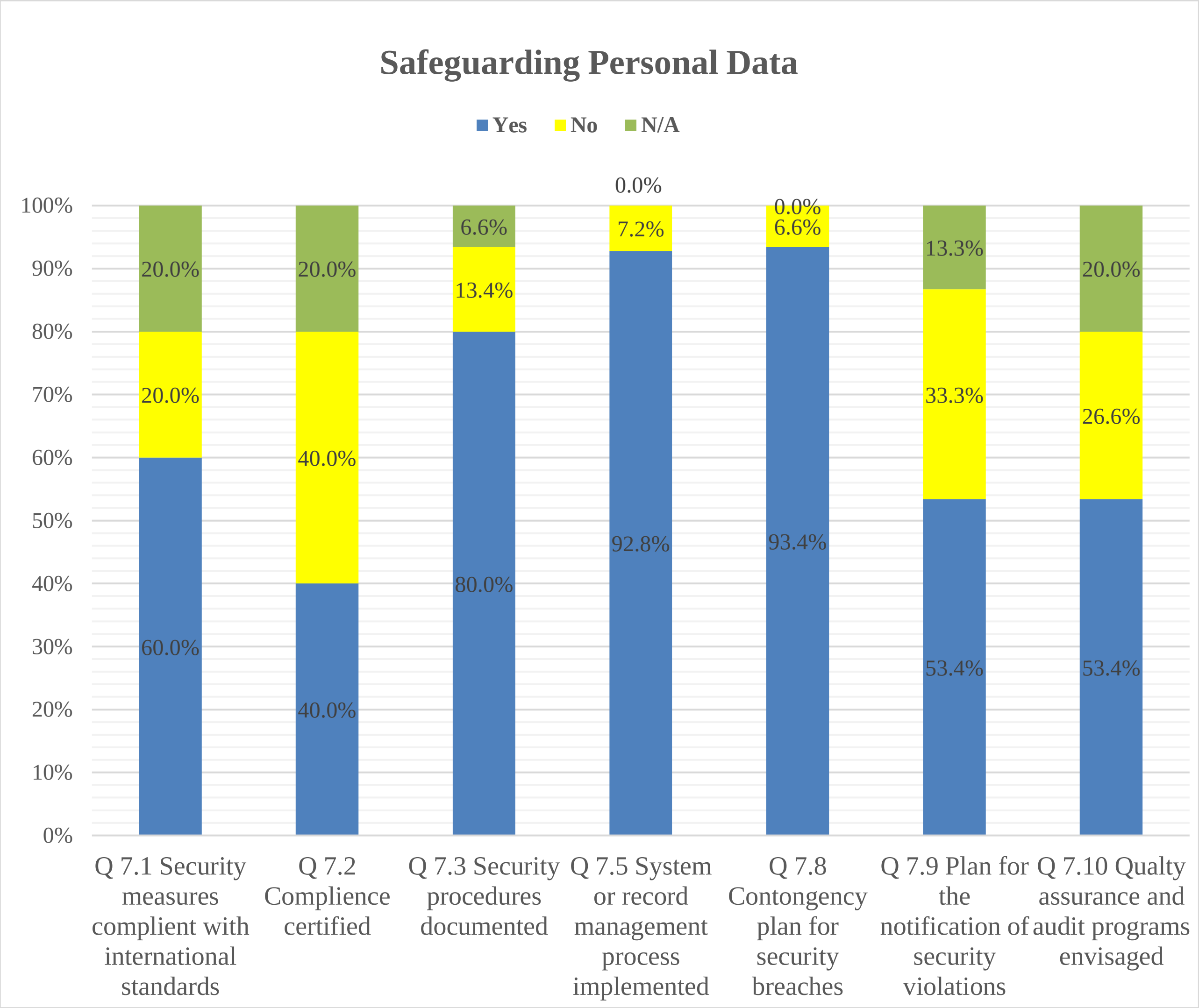


Figure 6: Safeguarding Personal Data

Section 8: Anonymisation

Anonymous data means data which does not relate to an identified or identifiable natural person (data subject) or personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable using any reasonable means. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

Anonymisation is different from both Pseudonymisation and de-identification.

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person;

De-identification means the processing of personal data in such a manner that data cannot identify an individual directly or indirectly. De-identification requires the removal of name and exact address; and can also involve the removal of any other detail or combination of details that might support identification.

The selected questions for this factor are as follows:

- Q 8.1: When anonymisation is required for the further processing of personal data contained in the registry/database/information system, is a standard anonymisation procedure envisaged?
- Q 8.2: If yes, is the applied procedure compliant with international technical standards and continuously updated according to the state of the art?
- Q 8.3: If yes, is the anonymisation process performed in compliance with the Data Protection Principles; for instance, performed confidentially, providing information to patients about the processing operation, applying security mechanisms for data storage and retention, etc.?
- Q 8.4: Is the anonymisation process documented?
- Q 8.5: Are anonymisation techniques implemented aimed to minimize all of the following risks: a) Singling out; b) Linkability; c) Inference?
- Q 8.9: Are anonymisation techniques/mix of techniques being implemented disclosed (e.g. made available to the public), especially when it is envisaged the release of the anonymised dataset?

.Four centres out of the 15 involved in the study found this section not applicable to them; e.g. anonymization process performed by a different entity. Hence, the following results are based on a sample of 11 centres.

Results highlight that when anonymisation is required for the further processing of personal data, a standard anonymisation procedure is envisaged the 66.7% of the sample, while it is not required in the 6.6% of cases.

The applied procedure is compliant with international technical standards and continuously updated according to the state of the art in the 81.8% of centres.

The anonymisation process is performed in compliance with the Data Protection Principles, documented and aimed to minimize the risks of singling out, linkability and inference in the 72.7% of cases.

The anonymisation techniques/mix of techniques implemented are instead disclosed only in the 18.2% of cases.

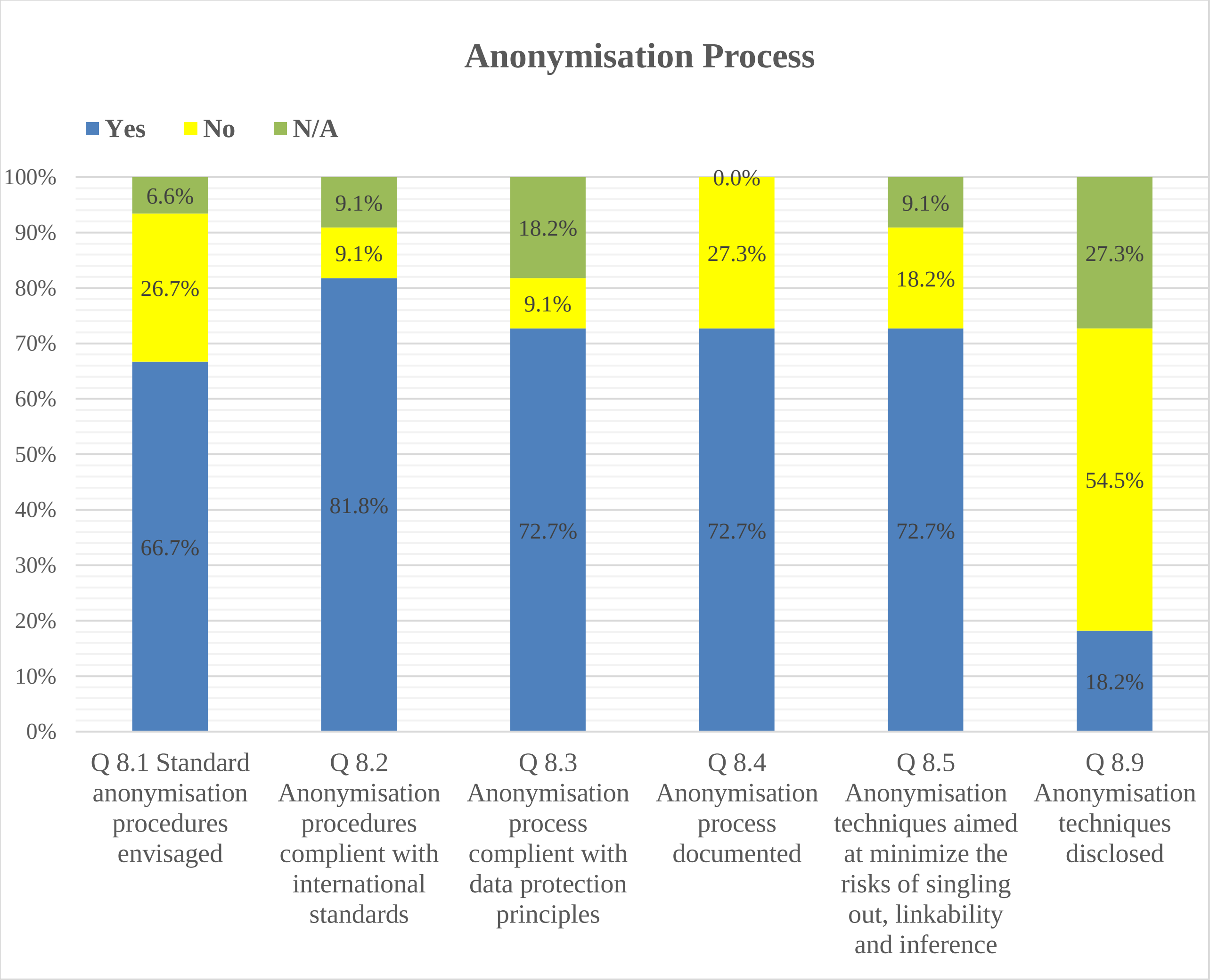


Figure 7: Anonymisation Process

5.1.2 PEIPA Factors Results

This section reports in detail the results obtained by participating centres for all key privacy/data protection and ethics factors (e.g. responsibility for personal data, consent, etc.) identified in the context of the BRIDGE-Health Privacy and Ethics Impact and Performance Assessment Step 1.

These key elements/factors constitute the 11 sections of the PEIPA questionnaire. The results obtained by the entire set of N=103 questions are extensive. To favour interpretation, results have been summarized by factor.

Each factor is composed of several questions (sub-factors) to which scores have been assigned according to the agreed scoring system. The sum of scores obtained in all sub-factors for a given factor provides an assessment of the privacy/data protection and ethics compliance with EU legislation and relevant principles and guidelines by factor.

The absolute values obtained as a sum of the individual components (questions, or sub-factors) are hereafter presented as standardized values, expressed as a percentage of the maximum score achievable for each factor. A graphical display of standardized values follows each sub-section.

The overall sample's compliance with privacy, data protection and ethics principles in each factor is evaluated according to the following scores:

Score	***Range***
Excellent	Median value ranges from 90% to 100%
Good	Median value ranges from 80% to 89%
Fair	Good: the median value ranges from 61% to 79%
Poor	Median value ranges from 40% to 60%
Very poor	Median value is equal or below the 39%

However the mean values and range of scores obtained by the sample in each factor is also taken into account.

Section 1. Responsibility for personal data

This section of the questionnaire refers to the accountability for personal data. This section is composed of 13 questions (sub-factors) that aim to assess:

- If data controllers are nominated and, if yes, if they have determined the purpose and means of data processing
- If a data protection policy has been implemented by data controllers
- If measures to implement privacy by design, by default and the data minimization principle are envisaged
- If privacy/data protection impact assessments are conducted
- If measures that ensure accountability are documented

Results for this factor are fairly homogeneous. Indeed, the highest score (Max Score=13) was reached only by the 20 % of the registries/databases/information systems involved. The 66.6% of centres scored above the mean value of the sample (84%); while the median value riches the 92% of the maximum score, which highlights an excellent overall compliance with privacy/data protection principles for this factor. The range of scores spans from 62% to 100%.

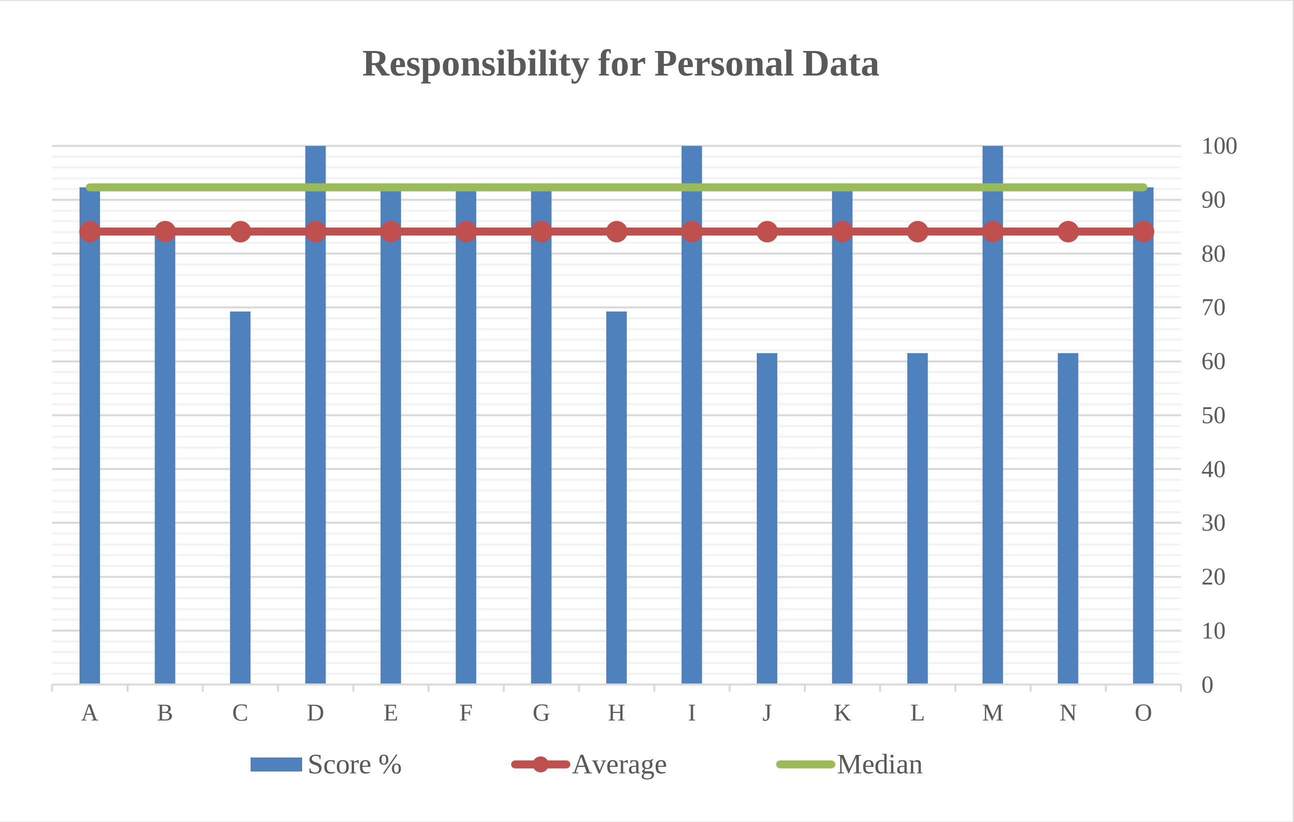


Figure 8: Responsibility for Personal data

Section 2: Collection and Use of Personal Data

This section of the questionnaire investigate on the collection and use of personal information. It is composed of 10 questions (sub-factors).

Questions are aimed to assess:

- if centres have a legal base for the collection and use of personal data
- if collection is performed with the data subject consent
- if personal data are collected according to the minimization principle
- if compatible secondary uses of personal data are allowed
- if data is de-identified and/or pseudonymised before it is used secondary purposes, including data-linkage
- if information is anonymised before being used for planning, management and/or evaluation purposes

Results for this factor are homogenous. Responses show that the 33.3% of the sample obtained the maximum score for this factor; which is the same proportion of the sample that scored above the average value (91%); while the median value is 90%, which highlights an excellent overall compliance with privacy/data protection principles for this factor. The range of scores spans from 80% to 100%.

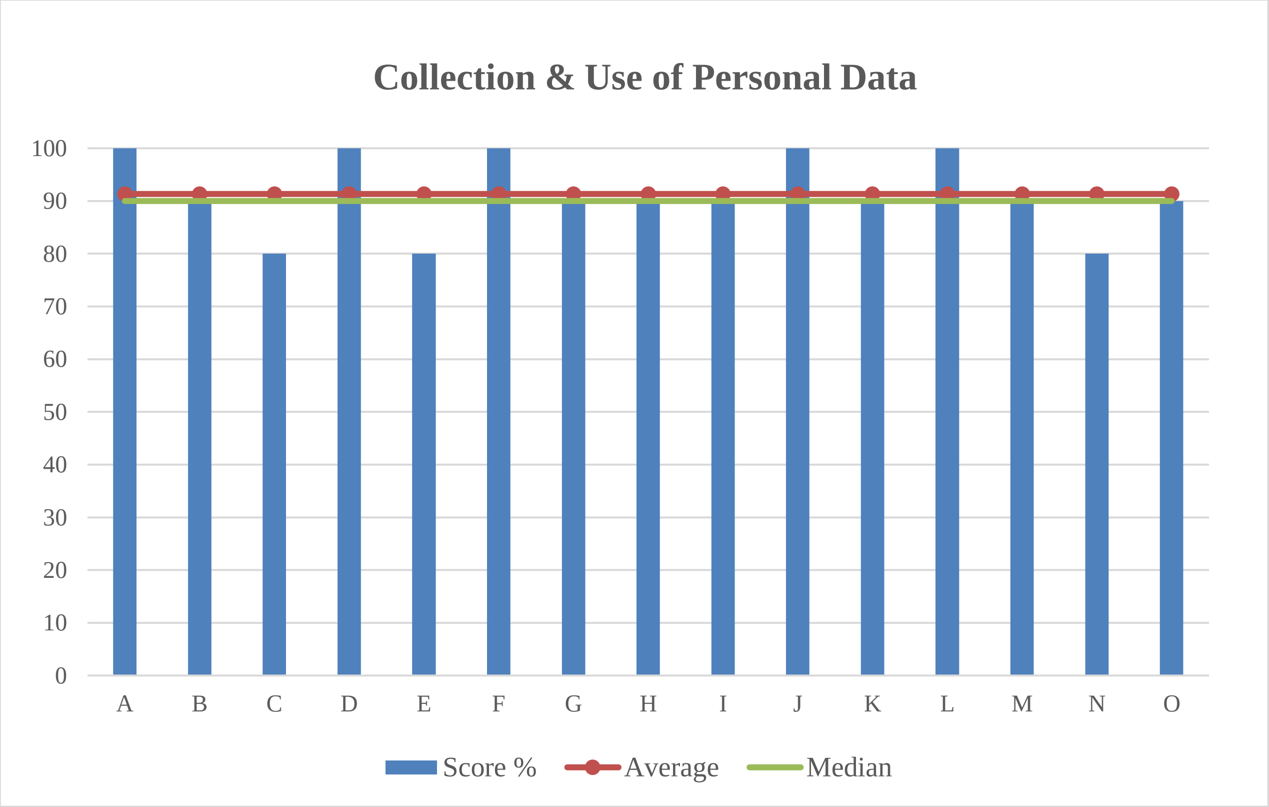


Figure 9: Collection and Use of Personal Data

Section 3: Consent

This section, composed of 10 questions (sub-factors) explores informed consent issues in order to determine:

- If consent is required for the collection and processing of personal data in the involved centres
- In case consent is required:
    - if it is obtained directly from the individual
    - if the data subject can refuse to consent to the use of his/her personal information for secondary purposes
    - if consent is given for one or more specified purposes
    - if a broad consent for further uses is allowed for approved health studies and research or for any other further uses
- In case consent is not required:
    - If consent is waived by law
    - If the data subject can opt-out

Results for this factor are homogenous too. Responses show that the 21.4% of the sample obtained the maximum score for this factor; the 28.6% of the sample scored above the average value (77%); while the median value is 70%, which highlights a fair overall compliance with privacy/data protection principles for this factor. The range of scores spans from 70% to 100%.

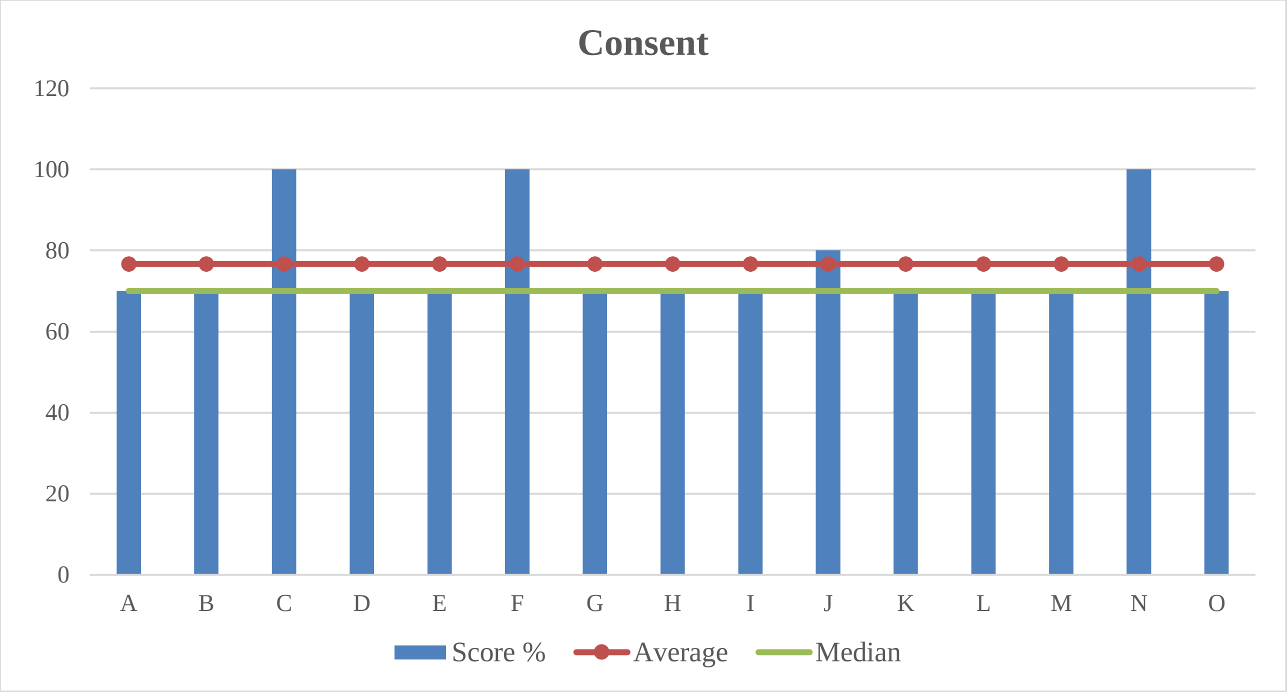


Figure 10: Consent

Section 4: Data Sharing

This section, composed of 8 questions (sub-factors), is aimed at analysing how information is shared within the BRIDGE-Health participating centres. Questions are intended to evaluate:

- If data controllers are allowed to share readily identifiable or de-identified health data for statistics or research with public authorities and/or academic or private organisations for non-commercial purposes
- If data controllers are allowed to share readily identifiable or de-identified/speudonymised health data for statistics or research with foreign public authorities and or academic or private organisations for non-commercial purposes (cross-border data flow)
- If data controllers use a standard data sharing agreement for disclosing data, or multiple standard ones for different types of data requestors

Results for this section are fairly homogeneous. Only the 13.3% of the sample obtained the maximum score for this factor; however, the 60% of the sample scored above the average value (73%); while the median value is 75%. Although the range of scores spans from 50% to 100%, highlighting a more scattered distribution of scores/values if compared with previous factors, the median value show a fair compliance with privacy/data protection principles for this factor as well.

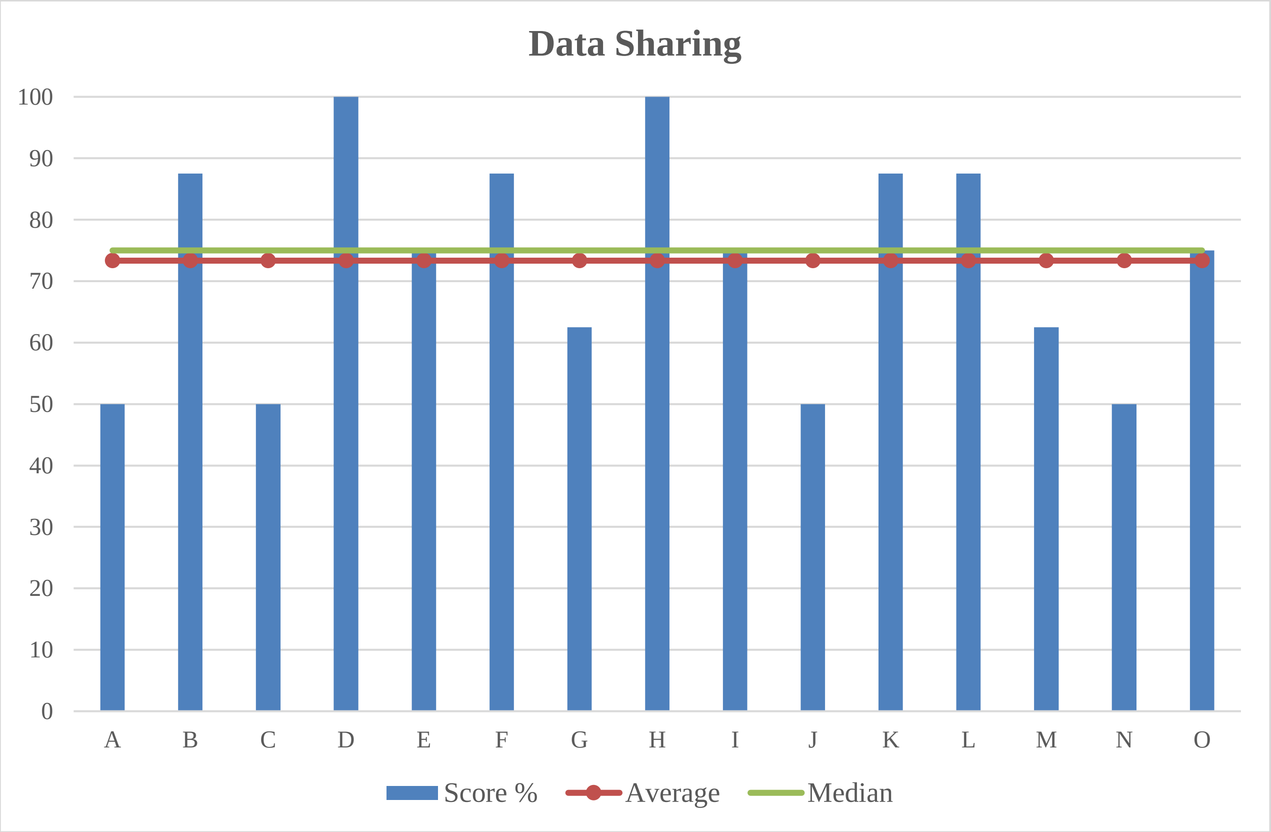


Figure 11: Data Sharing

Section 5: Data Linkage

This section is composed of 10 questions (sub-factors) and refers to specific issues relative to data linkage techniques. Questions are aimed to assess:

- Is record linkage is performed using the registry/database/information system records
- If unique personal identifiers, such as a social insurance number, are used for the purposes of linking across multiple databases (deterministic record linkage)
- If the registry/database/information system contains identifying attributes (such as name, sex, birth date, address) that could be used to link multiple sources (probabilistic record linkage)
- If standard practices for deleting direct identifiers (such as names and patient numbers) are used for the performance of data linkages
- If practices for creating pseudonyms from direct identifiers are applied
- If a standard process for the assessment of the risk of data re-identification is implemented
- Is the de-identification and/or pseudonymisation methodology is documented
- If standard practices for the treatment of attributes that pose a re-identification risk (such as rare diseases, exact dates, locations, or ethnic origins) are used.

Results for this section are heterogeneous. None of the centres obtained the maximum score for this factor. The 40% of the sample scored above the average value (51%), while the median value is 45%. Results highlight an overall poor compliance of the sample with privacy/data protection principles in this factor. The range of scores spans from 30% to 80%.

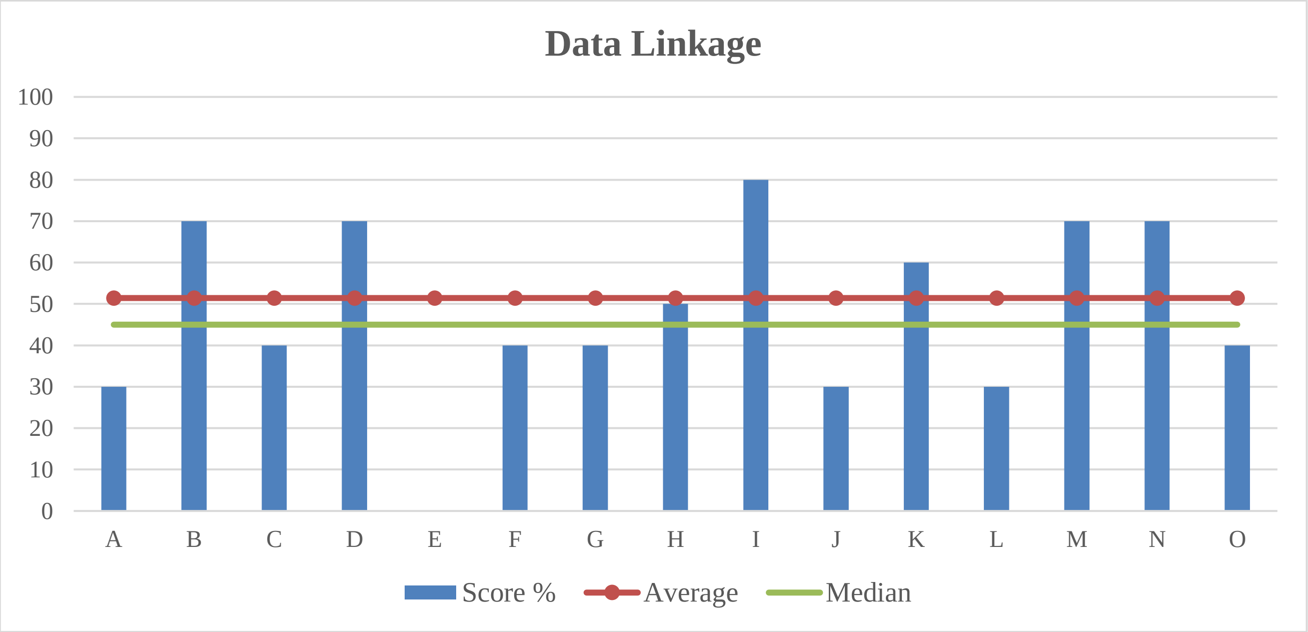


Figure12: Data Linkage

Section 6: Access and accuracy of Personal data

This section, composed of 10 questions (sub-factors), investigates on the accuracy of personal information and the possibility for individuals to access their records. To this end, questions aims to evaluate:

- If the registry/database/information system is designed to ensure that an individual can have access to his/her personal information
- If the registry/database/information system is designed to ensure that an individual can request the rectification or erasure of personal information
- If the registry/database/information system is designed to ensure that an individual can request the restriction of processing of personal data
- If the registry/database/information is system designed to ensure that an individual can object to the processing of personal data
- If the data controller provides the data subject access to personal data and information to the data subject (e.g. purpose of the processing, categories of data, recipients, storage duration)
- If there is a clearly defined process by which an individual may access, assess and discuss or dispute the accuracy of the record

Results for this factor show a high degree of heterogeneity. Only the 13.3% of centres obtained the maximum score. The 46.6% of the sample scored above the average value (46%); while the median value is 50%. For the 13.3% of the centres (N=2 centres) this section was not applicable. The mean and median values do not consider those values as =0 but as missing values. Hence, both mean and median values are calculated on a sample of 13 centres out of the 15 centres involved in the study. The range of scores spans from 0% (N=1 centres scored 0) to 100%. Results highlight an overall poor compliance of the sample with privacy/data protection principles in this factor.

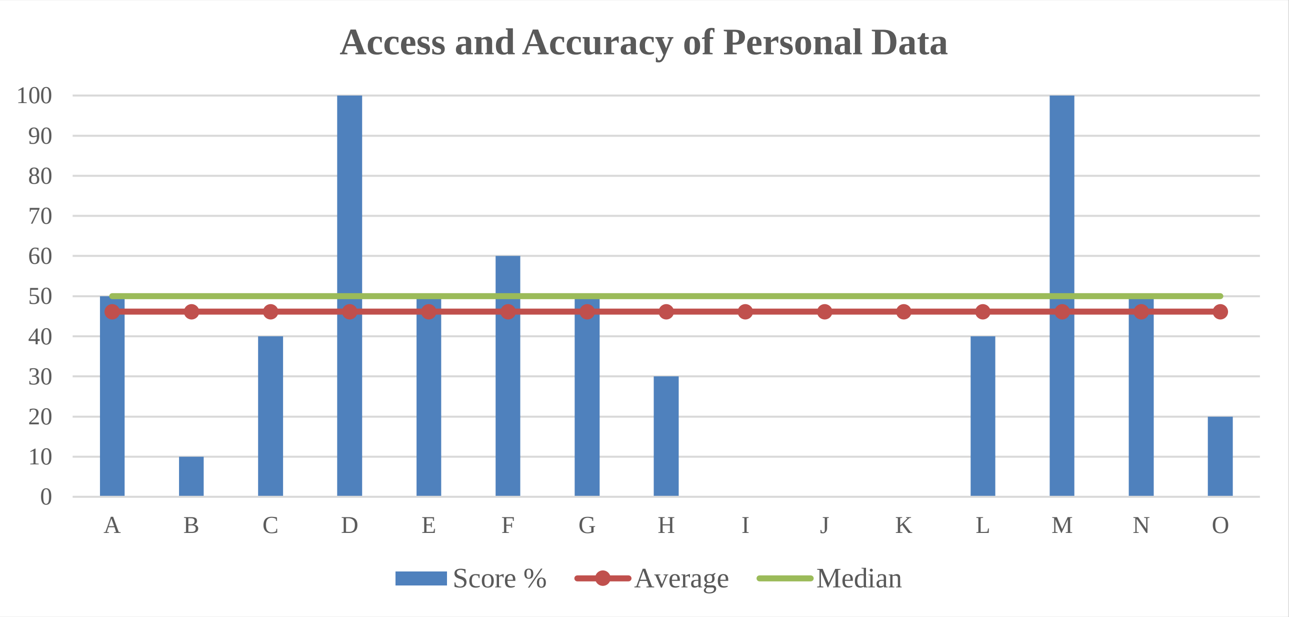


Figure 13: Access and Accuracy

Section 7: Safeguarding Personal Data

This section, composed of 10 questions (sub-factors), is concerned with security measures for safeguarding personal information.

Questions aim to ascertain:

- If security measures are compliant with international standard e.g. ISO 27001:2013, a standard for information security management; ISO 27002:2013, a catalogue of information security controls; ISO 27005:2011, a standard for information security risk management; or comparable standards
- If compliance with international standards is certified by accredited registration bodies (e.g. assessment and registration bodies, certification/ registration bodies or registrars)
- If security procedures are documented
- If user accounts, access rights and security authorizations are controlled by a system or record management process
- If contingency plans and documented procedures are in place to identify and respond to security breaches or disclosures of personal information in error
- If documented procedures are in place to communicate/notify security violations to the data subject, law enforcement authorities and relevant program managers when there is a risk to the rights and freedom of data subjects
- If personnel is trained on the requirements for protecting personal information and if they are aware of the relevant policies regarding breaches of security, integrity or confidentiality
- if security measures applied are commensurate to the sensitivity of information processed
- If there is a plan for quality assurance and audit programs to assess the ongoing state of the safeguards applicable to the system

Results for this factor are fairly heterogeneous. Only the 20% of centres obtained the maximum score. The 60% of the sample scored above the average value (69%); while the median value is 70%. The range of scores spans from 30% to 100%. Results highlights an overall fair compliance of the sample with privacy/data protection principles in this factor.

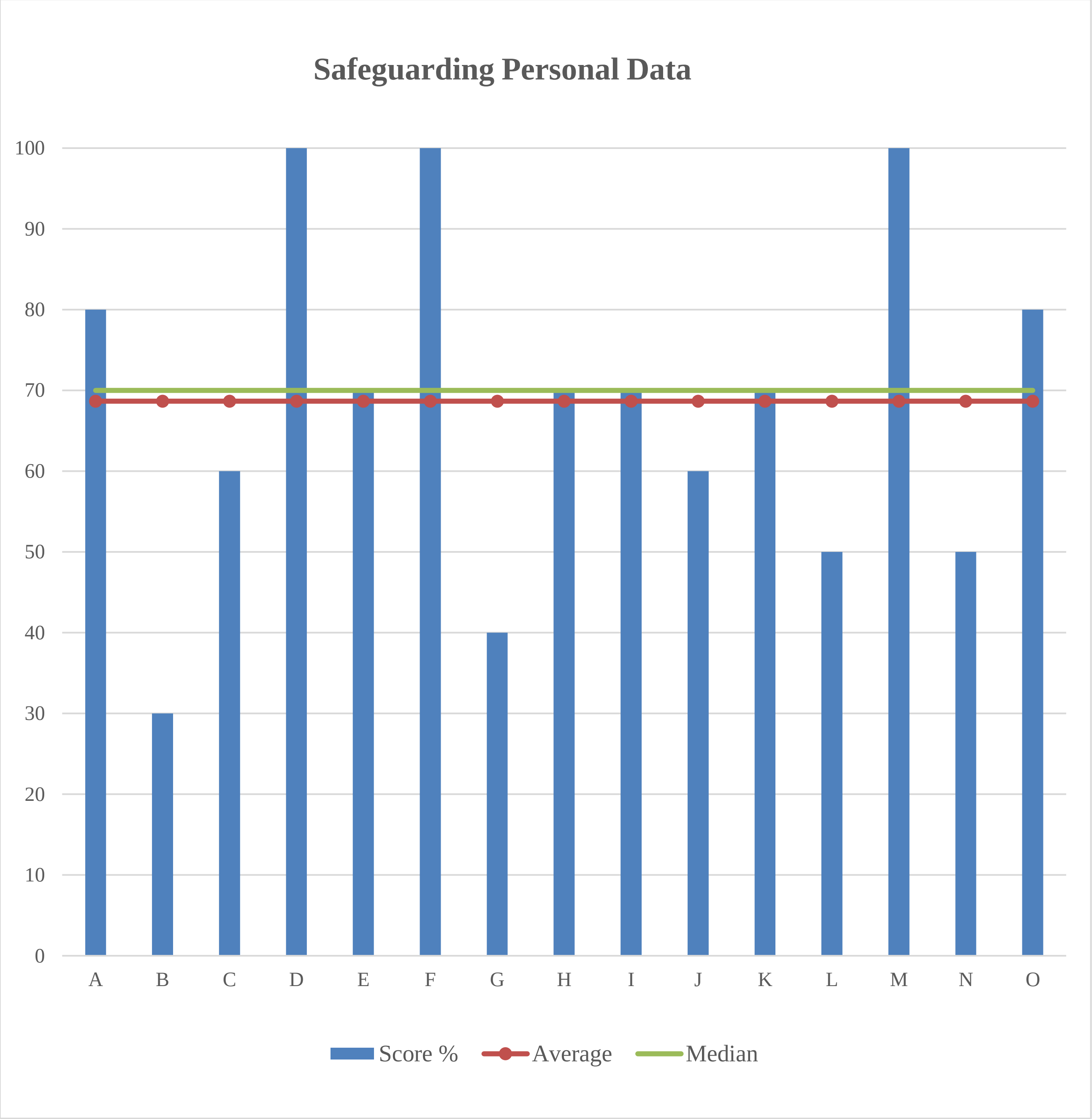


Figure 14: Safeguarding Personal Data

Section 8: Anonymisation Process

This section, composed of 9 questions (sub-factors), assesses the anonymisation process to ascertain:

- If a standard procedure is envisaged
- If it is compliant with international technical standards and continuously updated according to the state of the art
- If the anonymisation process is performed in compliance with the Data Protection Principles
- If the anonymisation process is documented
- If the anonymisation techniques implemented are aimed to minimize the risks of singling out, linkability and inference
- If anonymisation techniques/mix of techniques implemented are disclosed; e.g. made available to the public)

Results for this factor are highly heterogeneous. Only the 9.1% of centres obtained the maximum score. The 63.6% of the sample scored above the average value (55%); while the median value is 56%. For N=4 centres this section was not applicable. The mean and median values do not consider these values as =0 but as missing values. Hence, both mean and median values are calculated on a sample of 11 centres out of the 15 centres involved in the study. The range of scores spans from 11% to 100%. Results highlights an overall poor compliance of the sample with privacy/data protection principles in this factor.

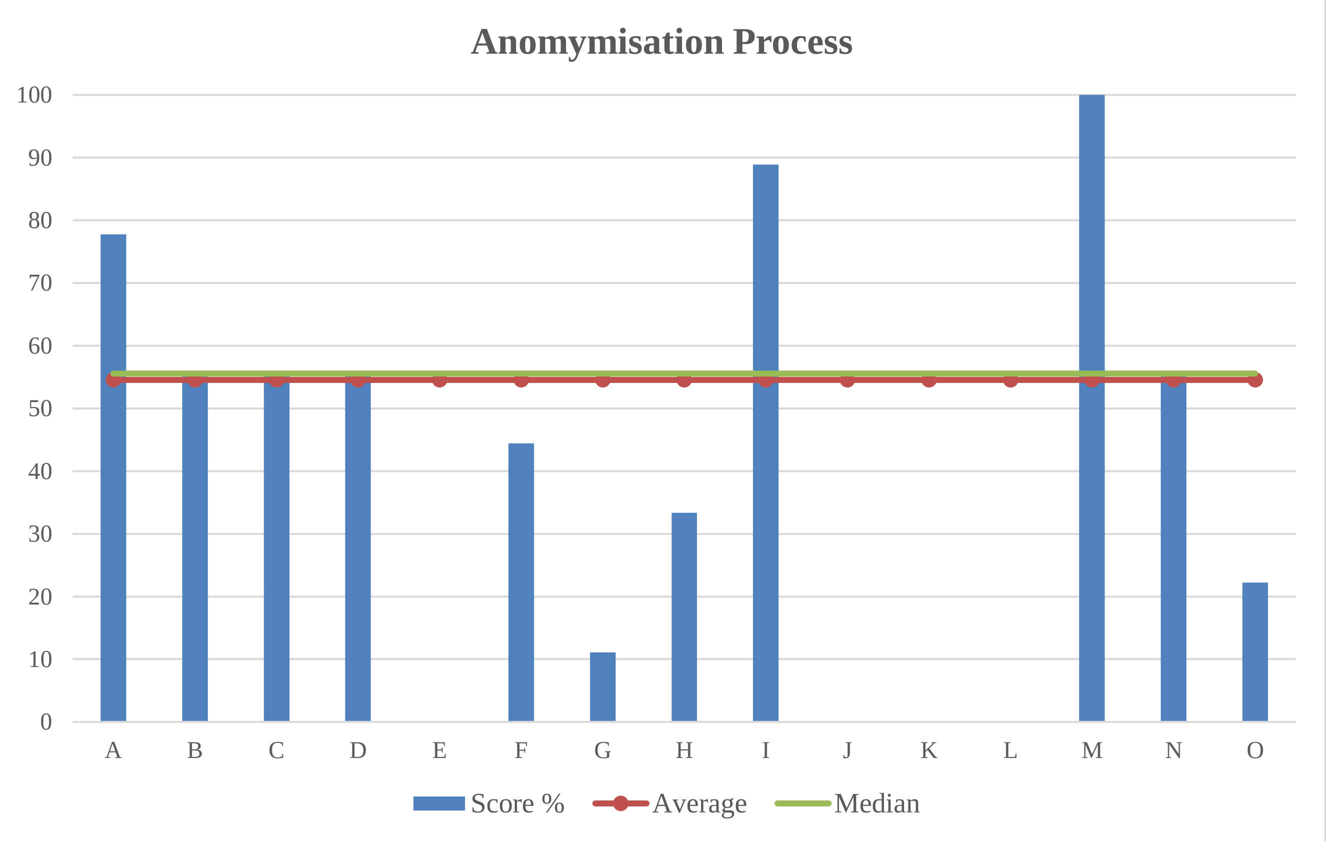


Figure 15: Anonymisation Process

Section 9: Openness, Transparency and public Engagement

This section, composed of 6 questions (sub-factors), relates to communication processes and strategies with the public. It is aimed to assess:

- If the public is consulted upon and informed about the collection and processing of health related data in the involved registries/databases/information systems
- If there is a communication plan to explain to the public how personal information will be collected, managed and protected
- If a certification/accreditation process for the processing of health data for research and statistics is implemented

Results for this factor are highly heterogeneous. Only the 18.2%% of centres obtained the maximum score. The 63.6% of the sample scored above the average value (58%); while the median value was equal to 67%. There were 4 cases in which the respondents considered the questions not applicable. The mean and median values do not consider these values as =0 but as missing values. Hence, both mean and median values are calculated on a sample of 11 centres out of the 15 centres involved in the study. The range of scores spans from 0% to 100%. Results highlights an overall fair compliance of the sample with privacy/data protection principles in this factor.

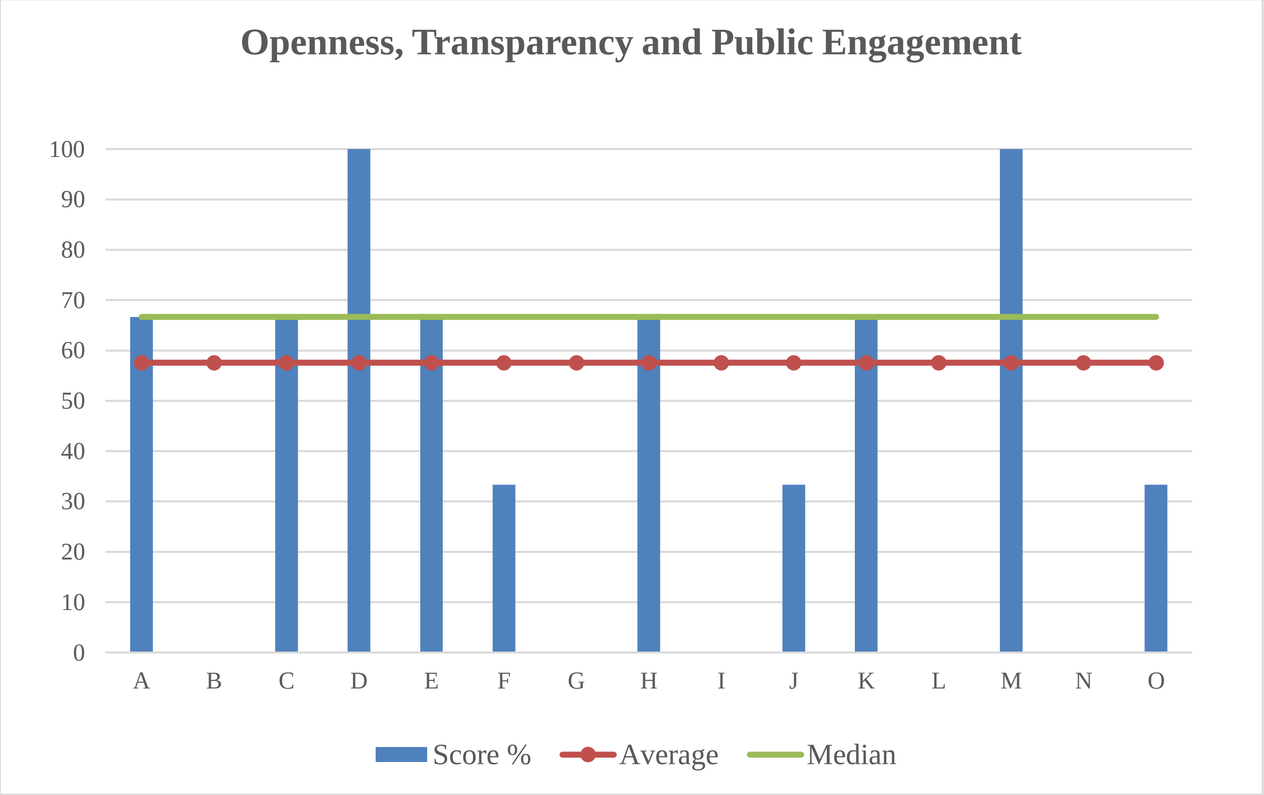


Figure 23: Openness, Transparency and Public Engagement

Section 10: Transparent Health Research Projects Approval Process

This section of the questionnaire, composed of 7 questions (sub-factors), is on the mechanisms implemented in project approval processes. It is aimed to evaluate:

- If research is authorized by a national/regional/local project approval bodies
- If project approval bodies are multidisciplinary
- If data controllers are involved (or consulted upon) in the project approval process
- If the criteria that the body follows for project approval are publicly identified, including timeliness of approval decisions
- If complaint procedures are envisaged to appeal against approval bodies' decisions

Results for this factor are fairly heterogeneous. However, only the 33.3% of centres obtained the maximum score. The 60% of the sample scored above the average value (70%), while the median value was equal to 71%. There were no cases in which the respondents considered the questions not applicable. The range of scores spans from 14% to 100%. Results highlights an overall fair compliance of the sample with relevant principles and guidelines in this factor.

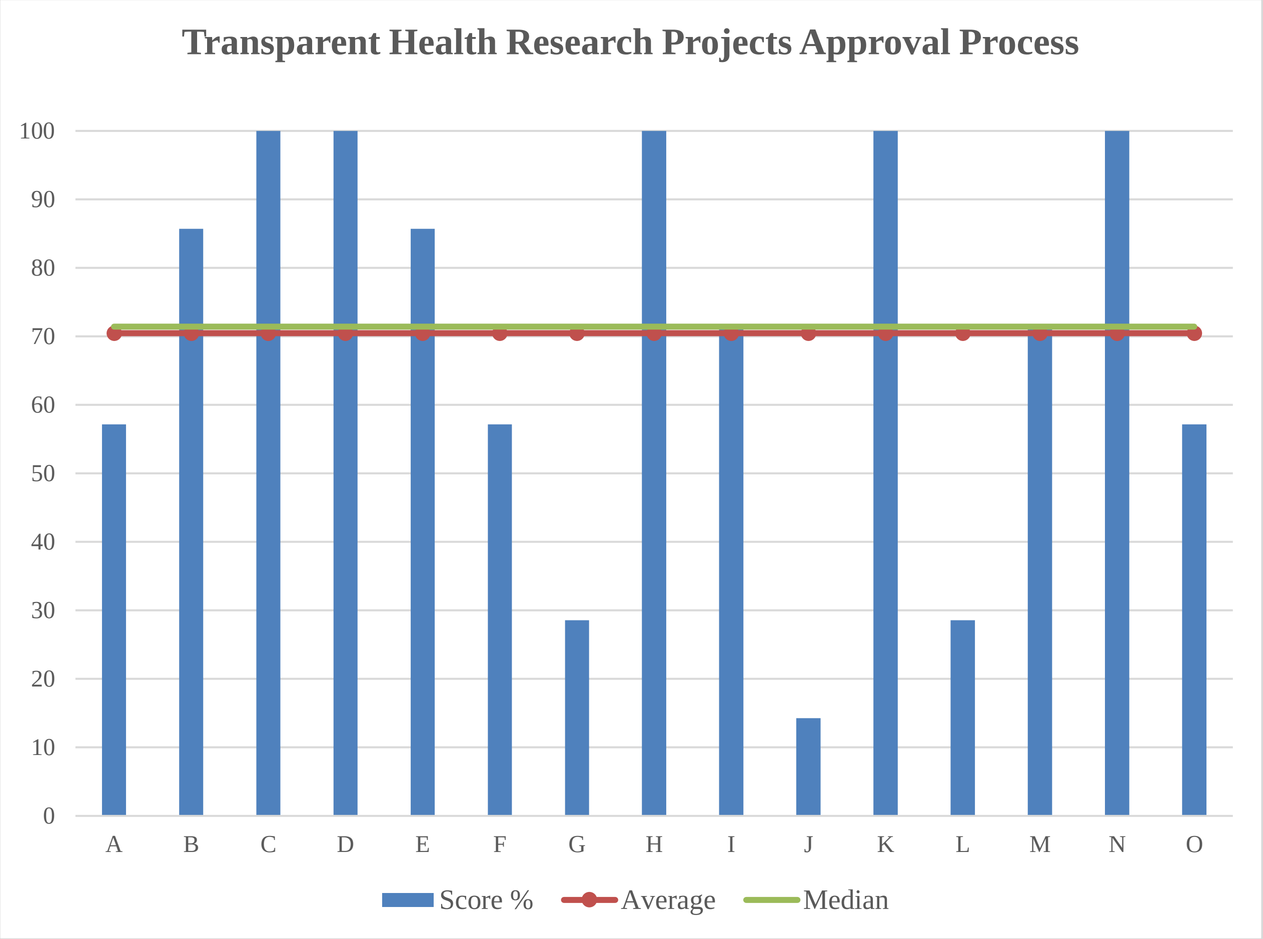


Figure 16: Transparent Health Research Projects Approval Process

Section 11: Beneficence/Non-maleficence Principles in Health Research Project Approval Processes

This section, composed of 10 questions (sub-factors), refers to the application of ethics principles in the project approval processes. Questions are aimed at assessing:

- If research projects are conducted using health related data contained in the registry/database/information system
- If they have to comply with protocols/guidelines/code of conduct that ensure that rights and dignity of patients are considered and respected
- If the burdens and potential harms of the research project are identified, considered, taken into account and documented
- If there are standard procedures to assess that burdens and potential harms, if any, are justified in the light of the potential benefit to participants and/or to society
- If project results are aimed to improve health outcomes, treatments, quality of health care, efficiency, cost or affordability of health care, the management or governance of the health sector, patients' health care experiences
- If the potential long term consequences of the research project are considered, addressed and documented
- If the potential for misuse (e.g. malevolent/criminal/terrorist abuse) is considered and, if any, addressed and documented

Results for this factor are fairly homogeneous. Although only the 13.3% of centres obtained the maximum score, the 60% of the sample scored above the average value (79%). The median values is equal to 80%. The range of scores spans from 50% to 100%. Results highlights an overall good compliance of the sample with relevant ethics principles in this factor.

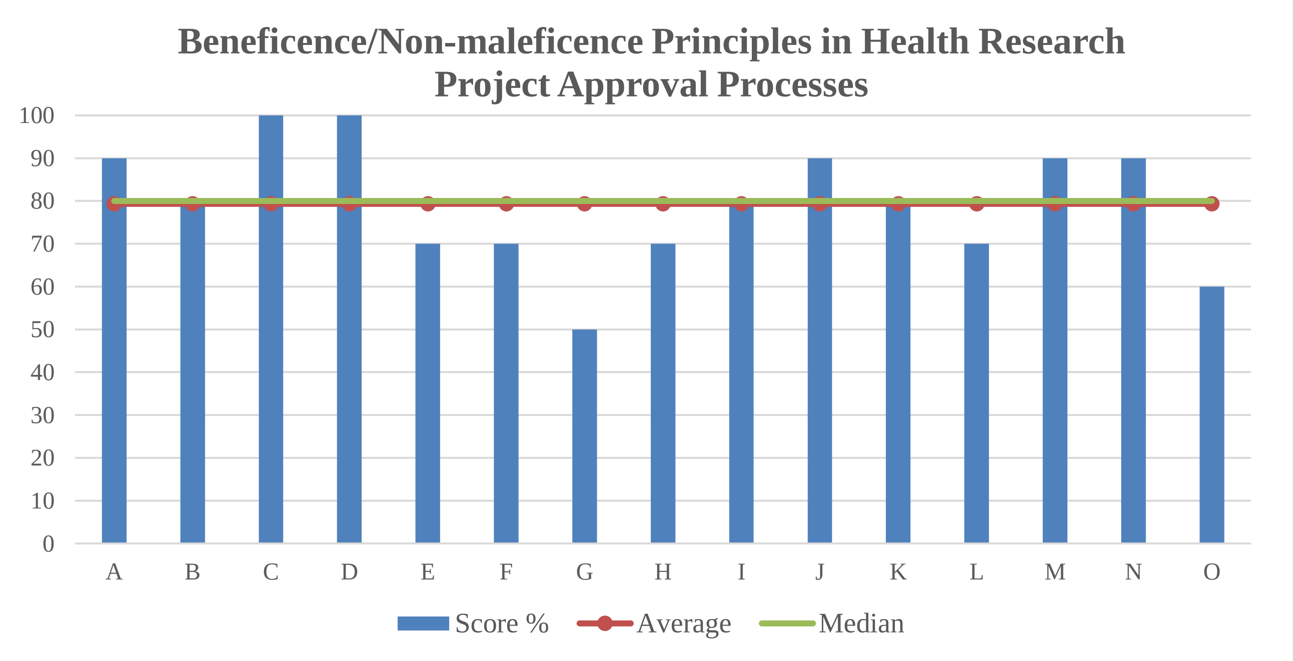


Figure 17: Beneficence/Non-maleficence Principles in Health Research Project Approval Processes

Standardized comparison of factor results

A standardized comparison of factor results, including the overall average as a percentage of the maximum attainable is presented in the below Table 1.

The analysis of median values allows to identify the areas that should be regarded as the most problematic. In fact, a "poor" performance, according to the scale of values agreed by the Panel of Experts (see page 26 of the present report), was identified in the following factors:

- Data Linkage (45%)
- Access and Accuracy (50%)
- Anonymisation (56%)

In the BRIDGE-Health sample, the following factors showed a high variability of scores (range):

- Data linkage (30%-80%)
- Access and accuracy of personal data (0%-100%)
- Safeguarding personal data (30%-100%)
- Anonymisation process (11%-100%)
- Openness, transparency and public engagement (0%-100%)
- Transparent health research projects approval process (14%-100%)
- Data sharing (50%-100%)
- Beneficence/Non-maleficence Principles in Health Research Project Approval Processes (50%-100)

Table 1: Standardized factors

Factor	Description	No.	Mean	Median	Range
A1	Accountability	13	84	92	62-100
A2	Collection and Use	10	91	90	80-100
A3	Consent	10	77	70	70-100
A4	Data Sharing	8	73	75	50-100
A5	Data Linkage	10	51	45	30-80
A6	Access & Accuracy	10	46	50	0-100
A7	Safeguarding	10	69	70	30-100
A8	Anonymisation	9	55	56	0-100
A9	Openness	6	58	67	0-100
A10	Project Approval process	7	70	71	29-100
A11	Beneficence	10	79	80	50-100

5.1.3 Overall Privacy/Data Protection and Ethics Performance

The average and median of scores obtained by the whole sample of BRIDGE-Health participating centres allows evaluating the overall level of privacy/data protection and ethics performance of the sample, observed against the highest attainable level of privacy protection and adherence to relevant ethical principles.

As shown in Figure 26, the highest **average** score (91%) was reached by the sample with regard to the factor “collection and use of personal data”, followed by “responsibility for personal data” (84%), “beneficence” (79%), “consent” (77%) and “data sharing” (73%).

Applying the same scale of values used for the assessment of the median values (see page 26 of the present report), it can be highlighted that the sample obtained median values between 80% and 100% (from “good” to “excellent” performance) in the following factors:

- Responsibility for PD
- Collection and Use of PD

The sample scored between 61% and 79% (“fair” performance) of the maximum score (mean values) in the following factors:

- Consent
- Data sharing
- Project approval process
- Beneficence

The sample scored below the 60% (mean values) in the following factors:

- Data linkage
- Access
- Anonymisation
- Openness

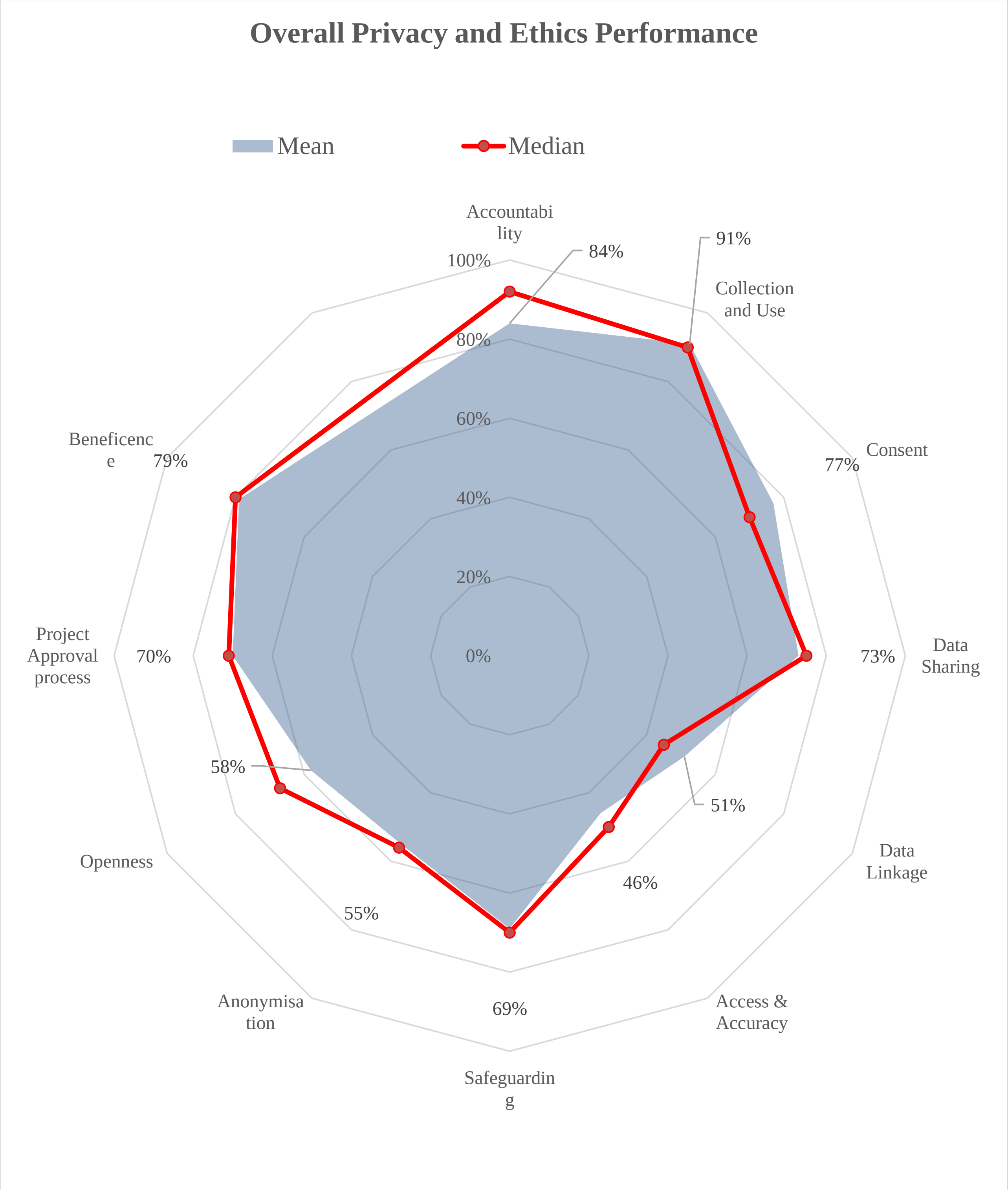


Figure 18: Overall Privacy and Ethics Performance of the BRIDGE-Health Sample

5.1.4 Privacy/Data protection and Ethics Performance by Consortia

The same graphical representation can be provided for each of the three consortia involved in the study. To this aim the mean values reported by the ECHO, EUBIROD and EUROHOPE consortia are hereafter presented for each factor analysed.

The light blue area highlights the mean results of the whole sample (sum of the three consortia results); while the red, violet and orange lines describe the results, by factor, of each consortia; respectively, ECHO, EUBIROD and EUROHOPE.

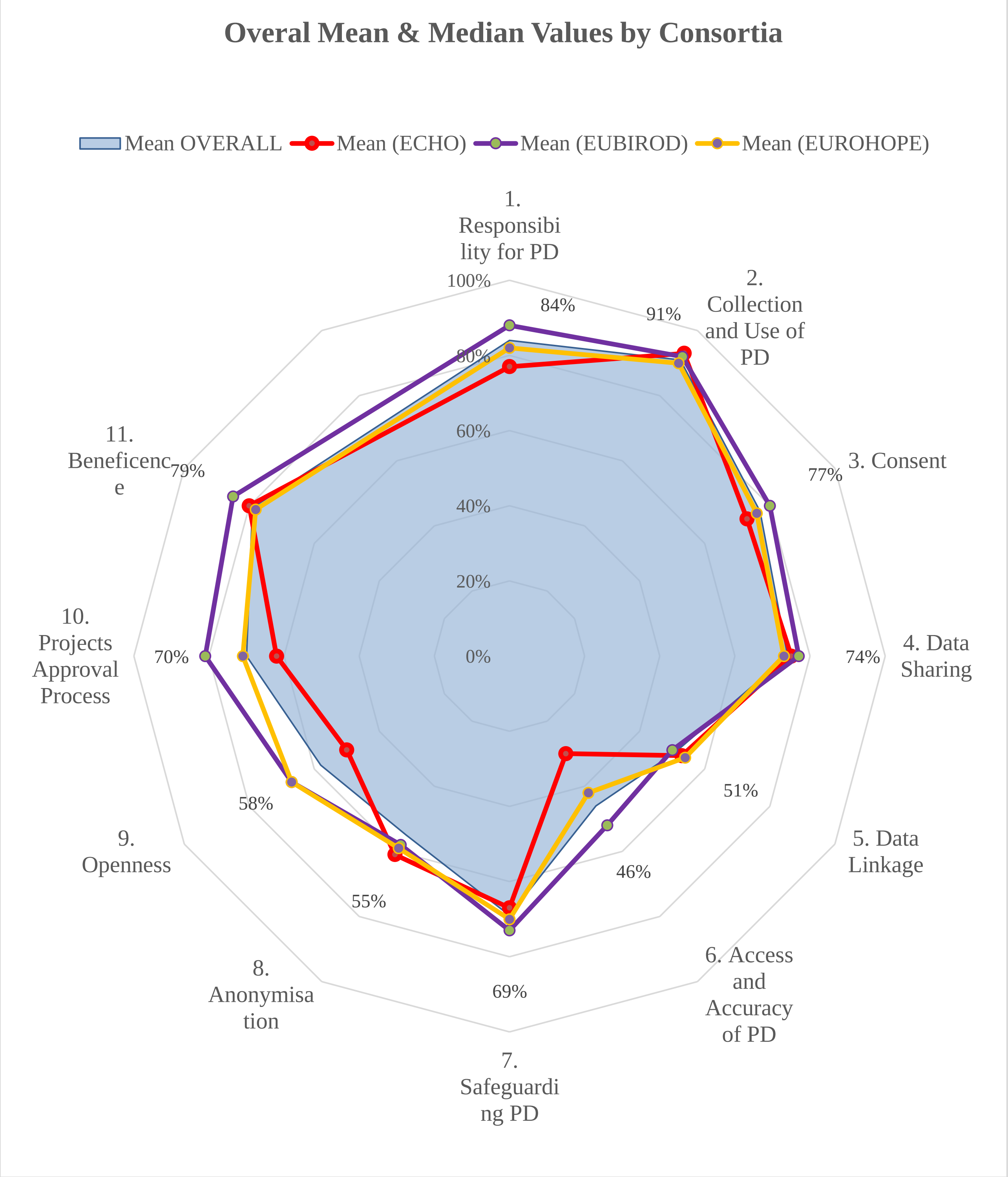


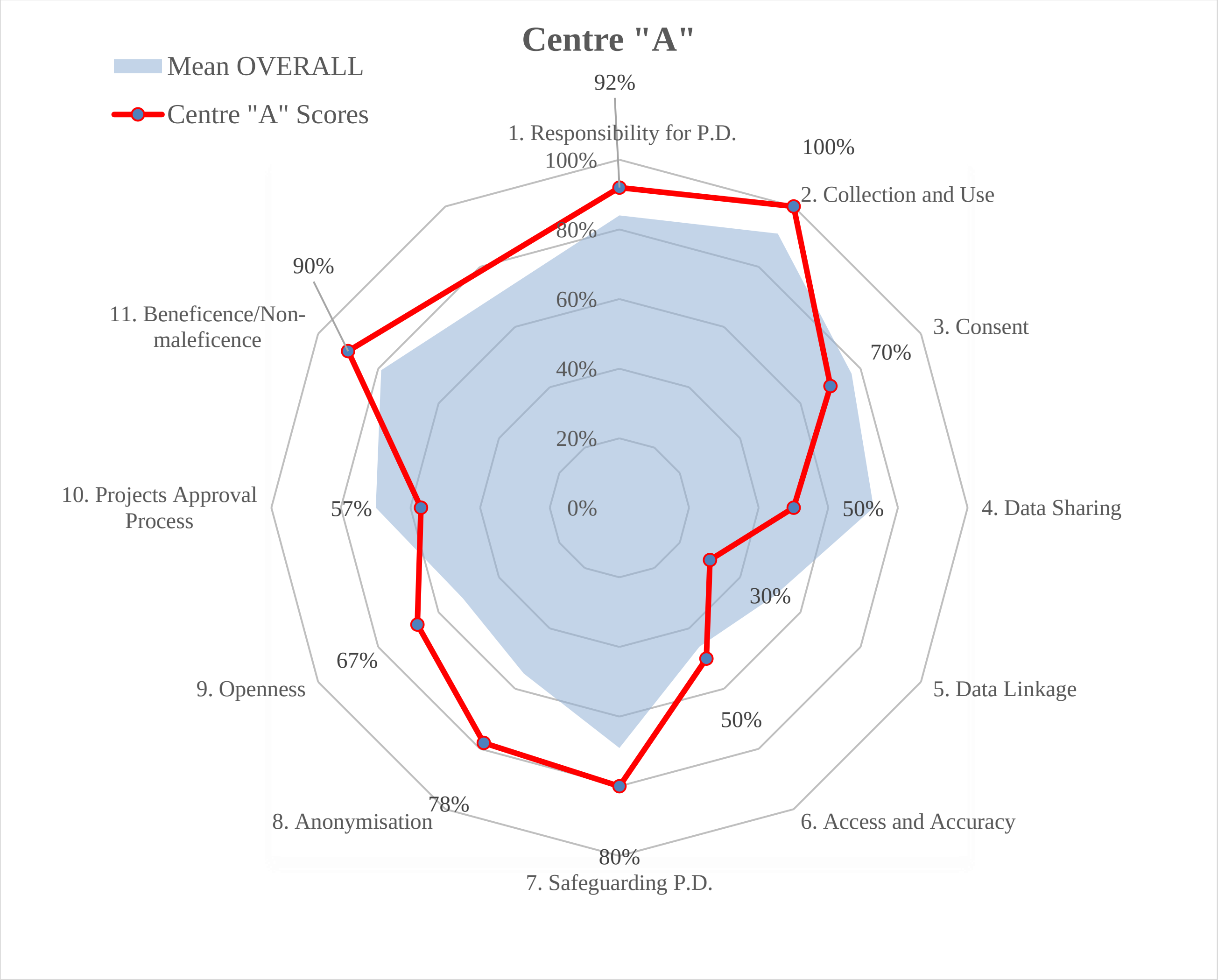
Figure 19: ECHO, EUBIROD and EUROHOPE performance by factor

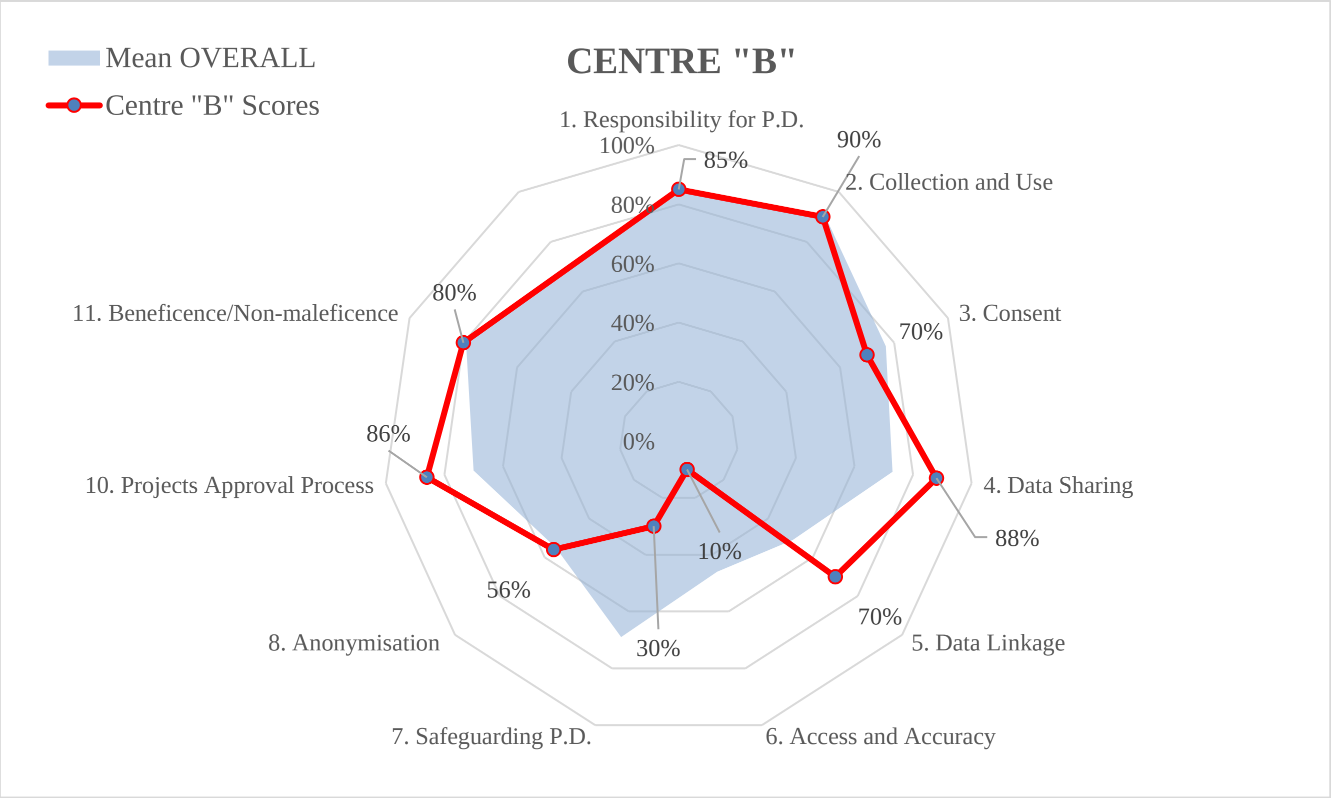
5.1.5 Privacy/Data protection and Ethics Profile of Participating Centre

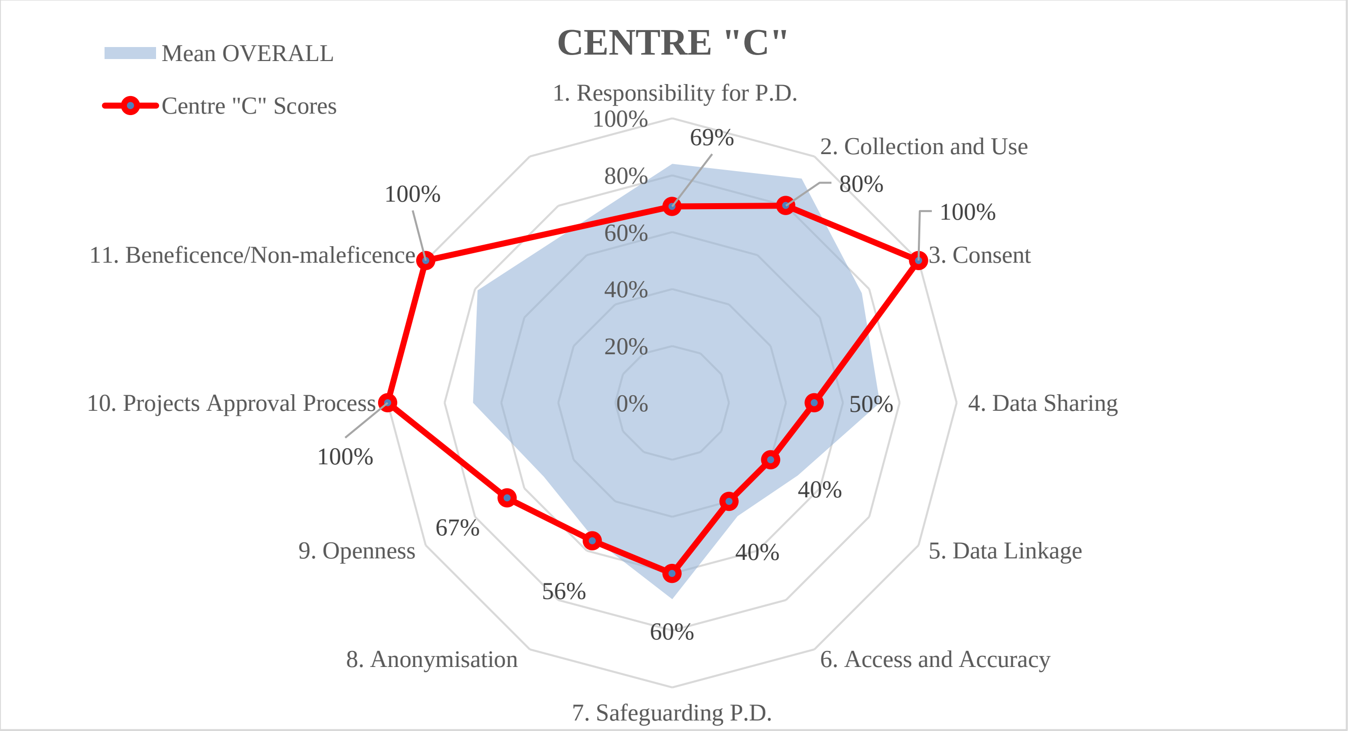
The following graphical representation provides, for each centre involved in the study, the scores (expressed as a percentage of the maximum attainable score) obtained in each of the 11 factors analysed.

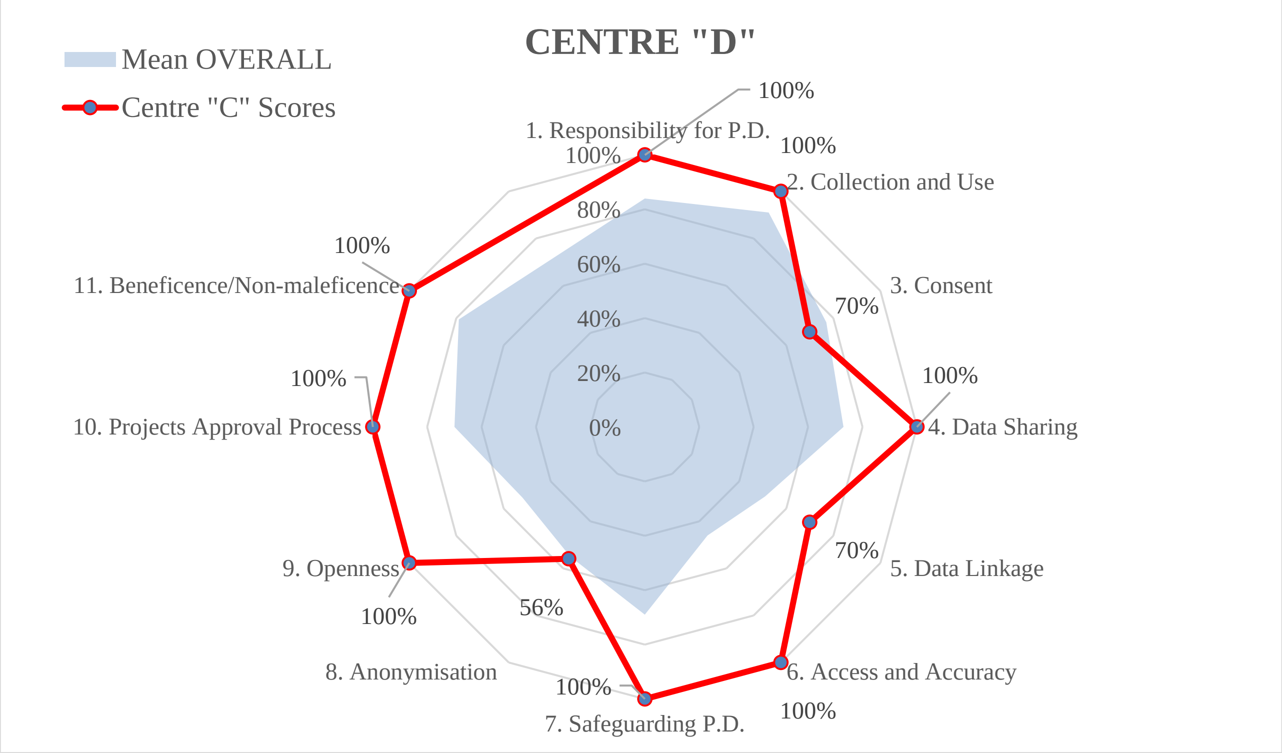
The light blue area represent the mean values of the entire sample.

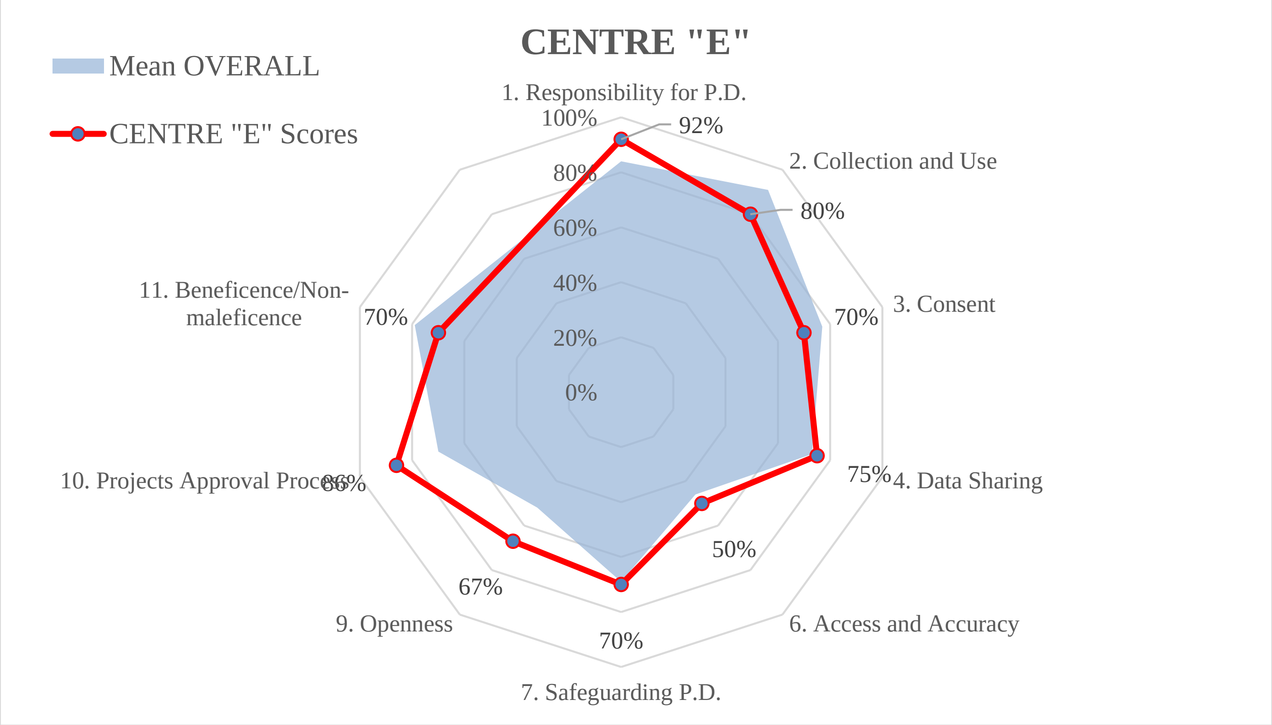
Hence, each centre can easily compare its privacy and ethics performance per factor both against the max attainable score and the sample's average.

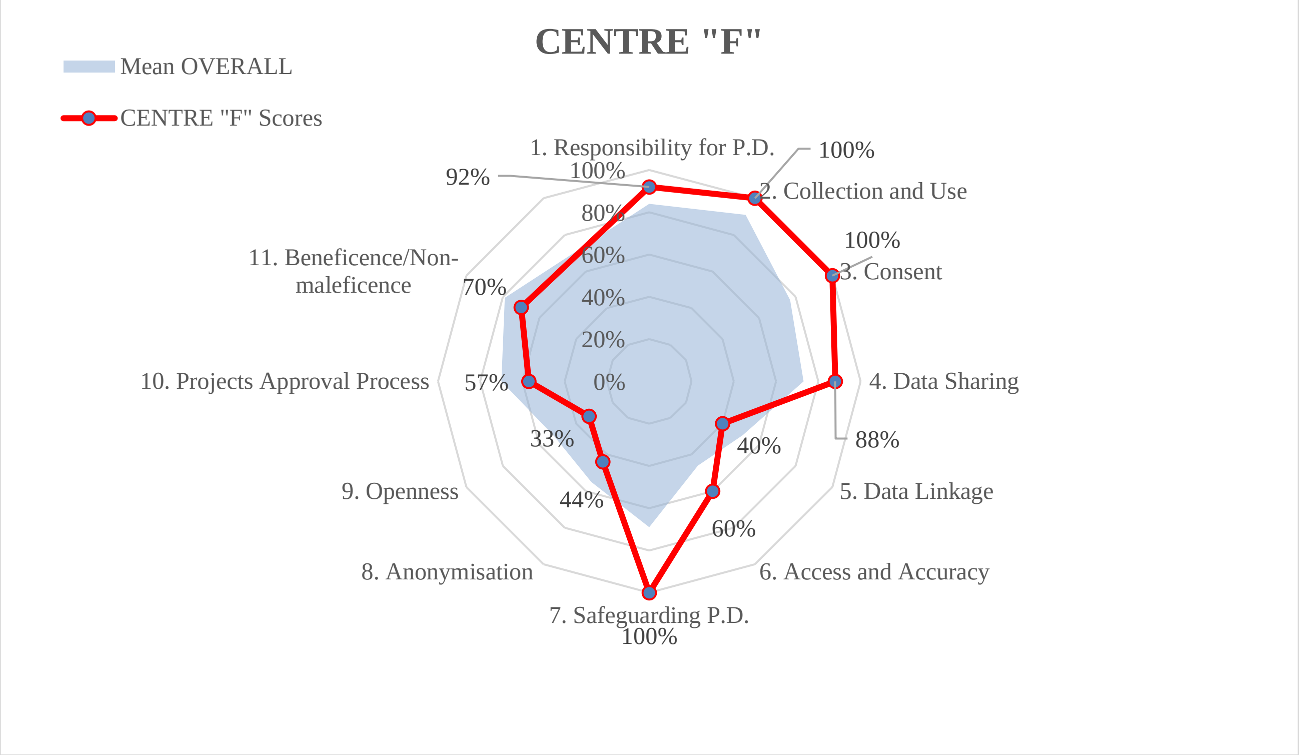


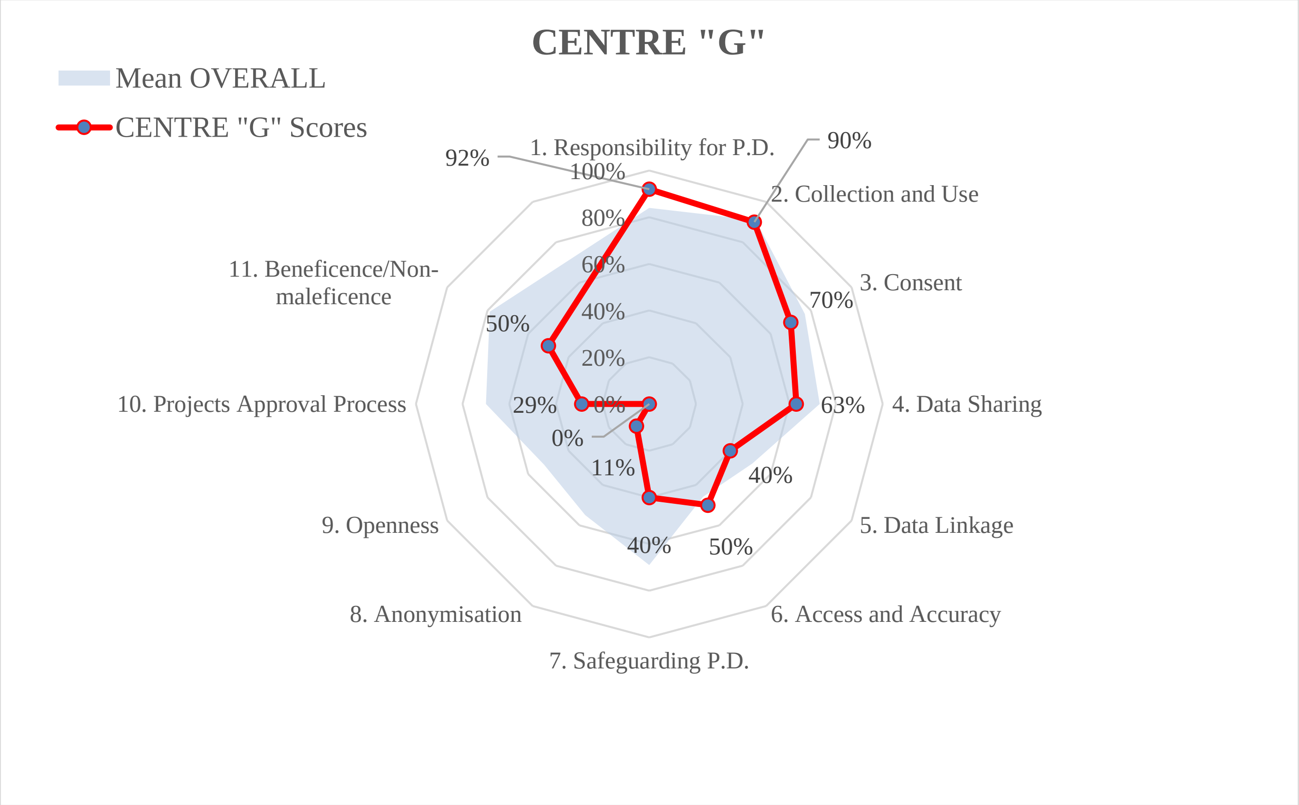

Mean OVERALL
Centre "B" Scores
CENTRE "B"
1. Responsibility for P.D.
2. Collection and Use
3. Consent
4. Data Sharing
5. Data Linkage
6. Access and Accuracy
7. Safeguarding P.D.
8. Anonymisation
10. Projects Approval Process
11. Beneficence/Non-maleficence
100%
80%
60%
40%
20%
0%
85%
90%
70%
88%
70%
10%
30%
56%
86%
80%

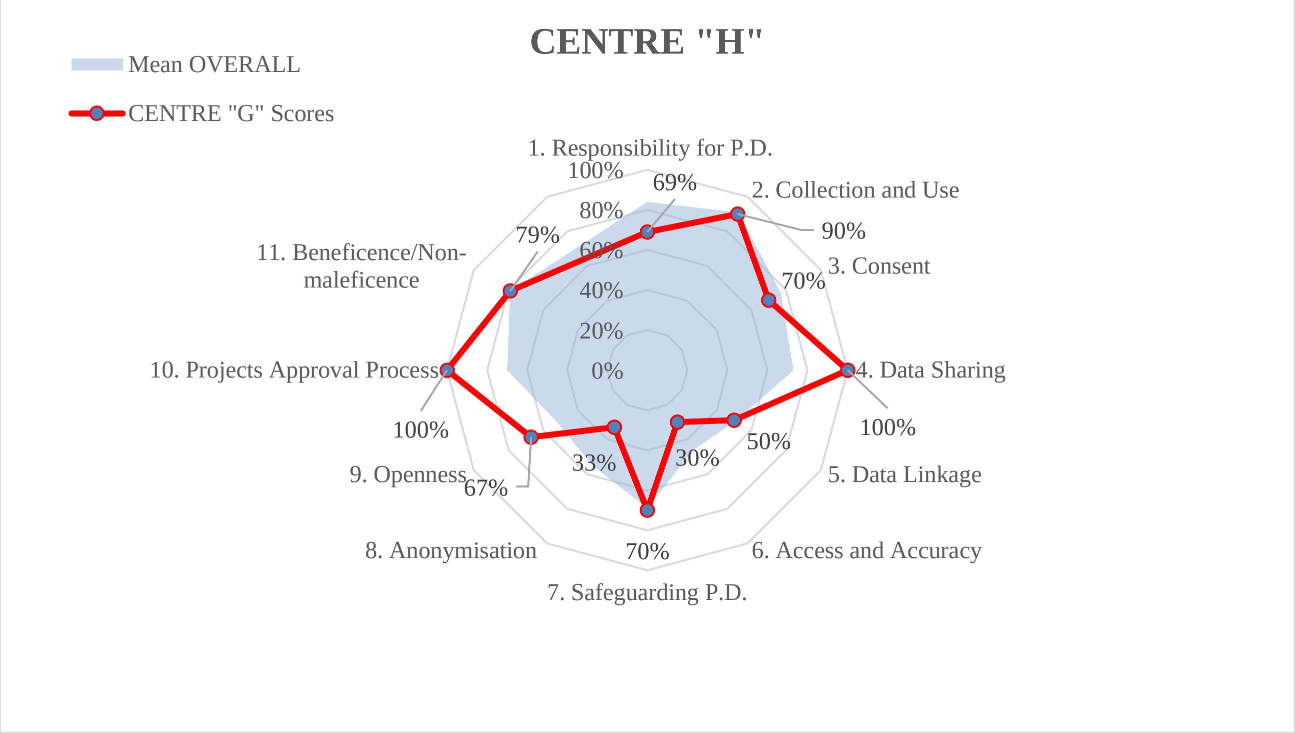

Mean OVERALL
Centre "C" Scores
CENTRE "C"
1. Responsibility for P.D.
2. Collection and Use
3. Consent
4. Data Sharing
5. Data Linkage
6. Access and Accuracy
7. Safeguarding P.D.
8. Anonymisation
9. Openness
10. Projects Approval Process
11. Beneficence/Non-maleficence
100%
80%
60%
40%
20%
0%
69%
80%
100%
50%
40%
40%
60%
56%
67%
100%
100%

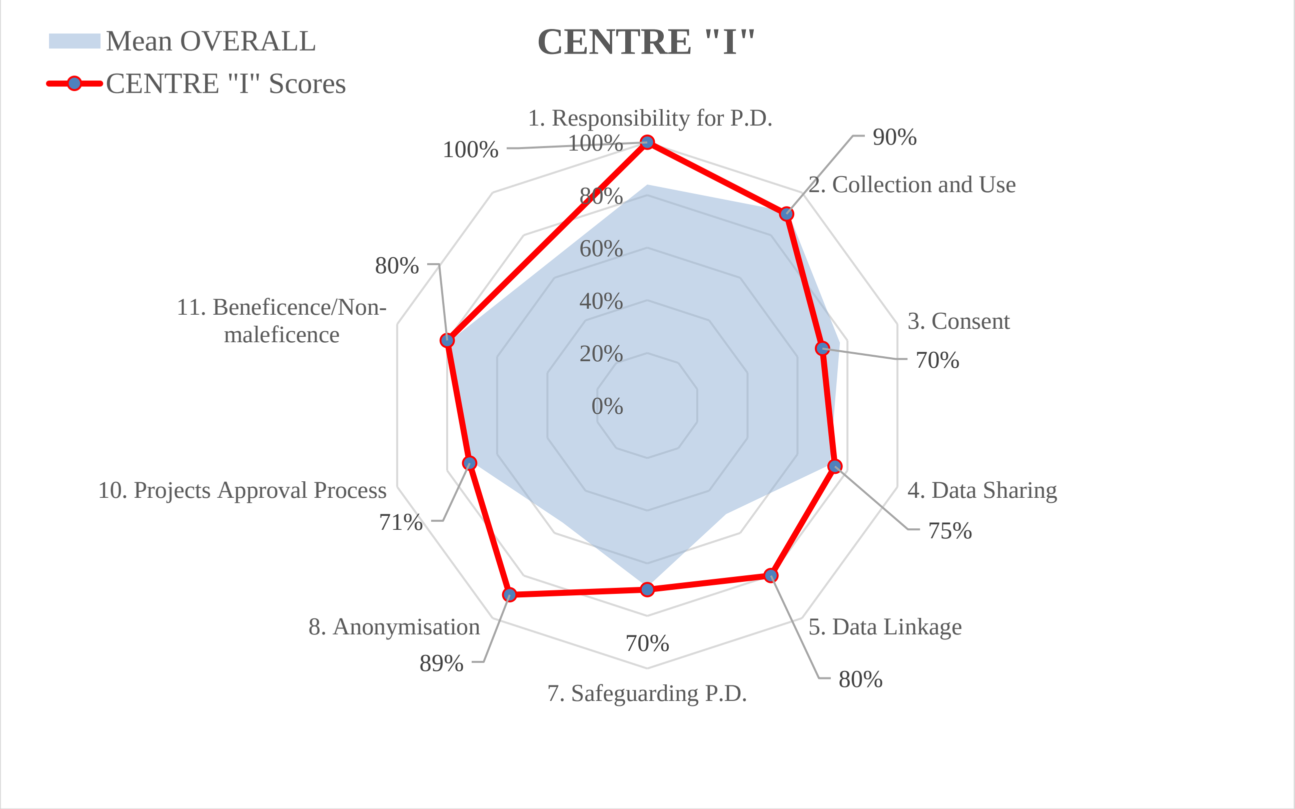

CENTRE "D"
Mean OVERALL
Centre "C" Scores
1. Responsibility for P.D.
2. Collection and Use
3. Consent
4. Data Sharing
5. Data Linkage
6. Access and Accuracy
7. Safeguarding P.D.
8. Anonymisation
9. Openness
10. Projects Approval Process
11. Beneficence/Non-maleficence
0%
20%
40%
60%
80%
100%
100%
100%
70%
100%
70%
100%
100%
56%
100%
100%
100%

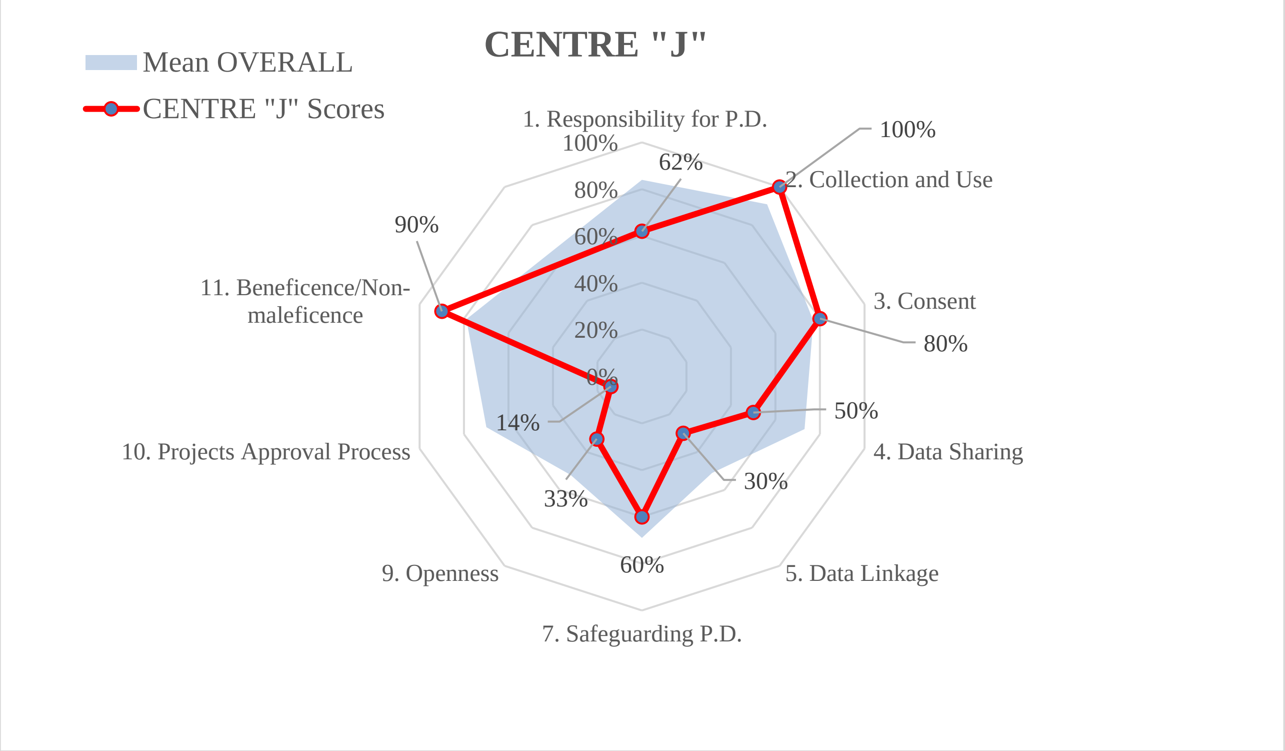

CENTRE "E"
Mean OVERALL
CENTRE "E" Scores
1. Responsibility for P.D.
2. Collection and Use
3. Consent
4. Data Sharing
6. Access and Accuracy
7. Safeguarding P.D.
9. Openness
10. Projects Approval Process
11. Beneficence/Non-maleficence
0%
20%
40%
60%
80%
100%
92%
80%
70%
75%
50%
70%
67%
86%
70%

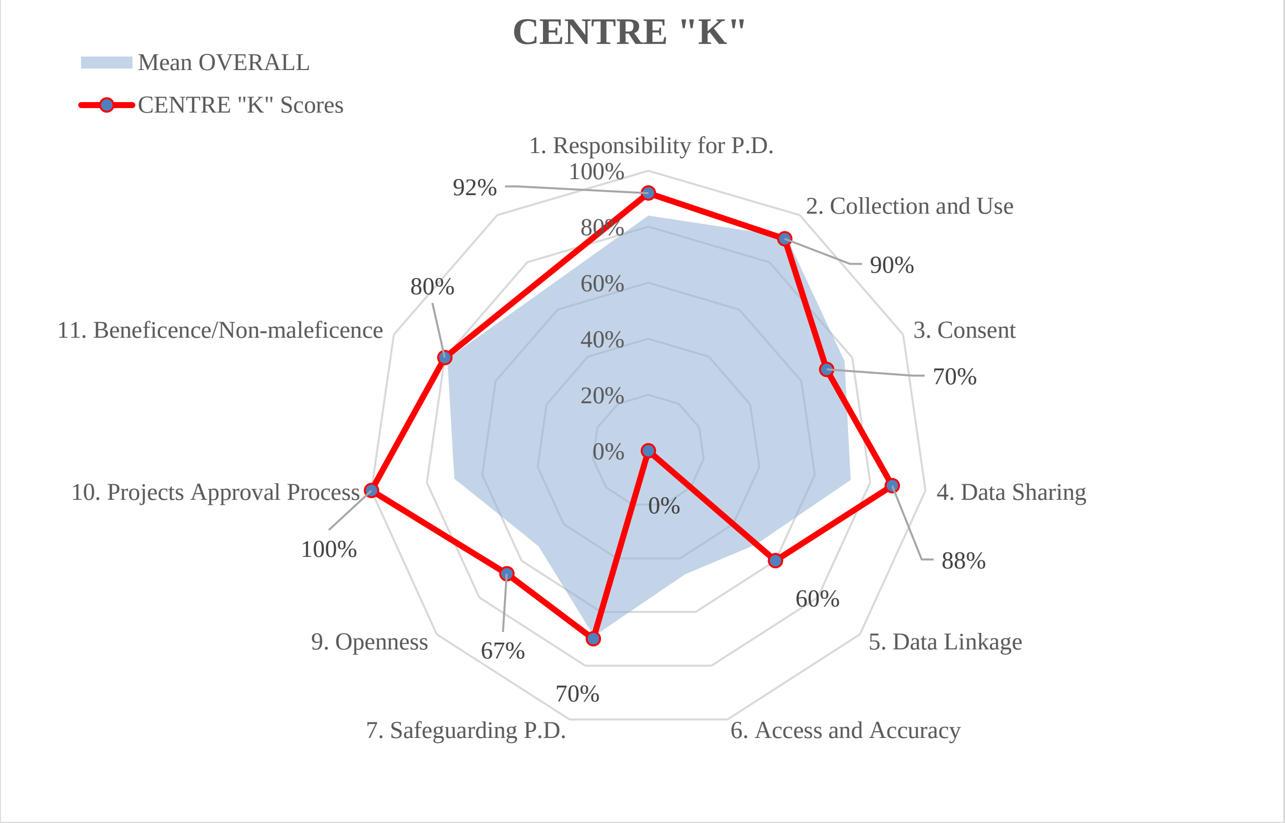

CENTRE "F"
Mean OVERALL
CENTRE "F" Scores
1. Responsibility for P.D.
2. Collection and Use
3. Consent
4. Data Sharing
5. Data Linkage
6. Access and Accuracy
7. Safeguarding P.D.
8. Anonymisation
9. Openness
10. Projects Approval Process
11. Beneficence/Non-maleficence
100%
80%
60%
40%
20%
0%
92%
100%
100%
88%
40%
60%
100%
44%
33%
57%
70%

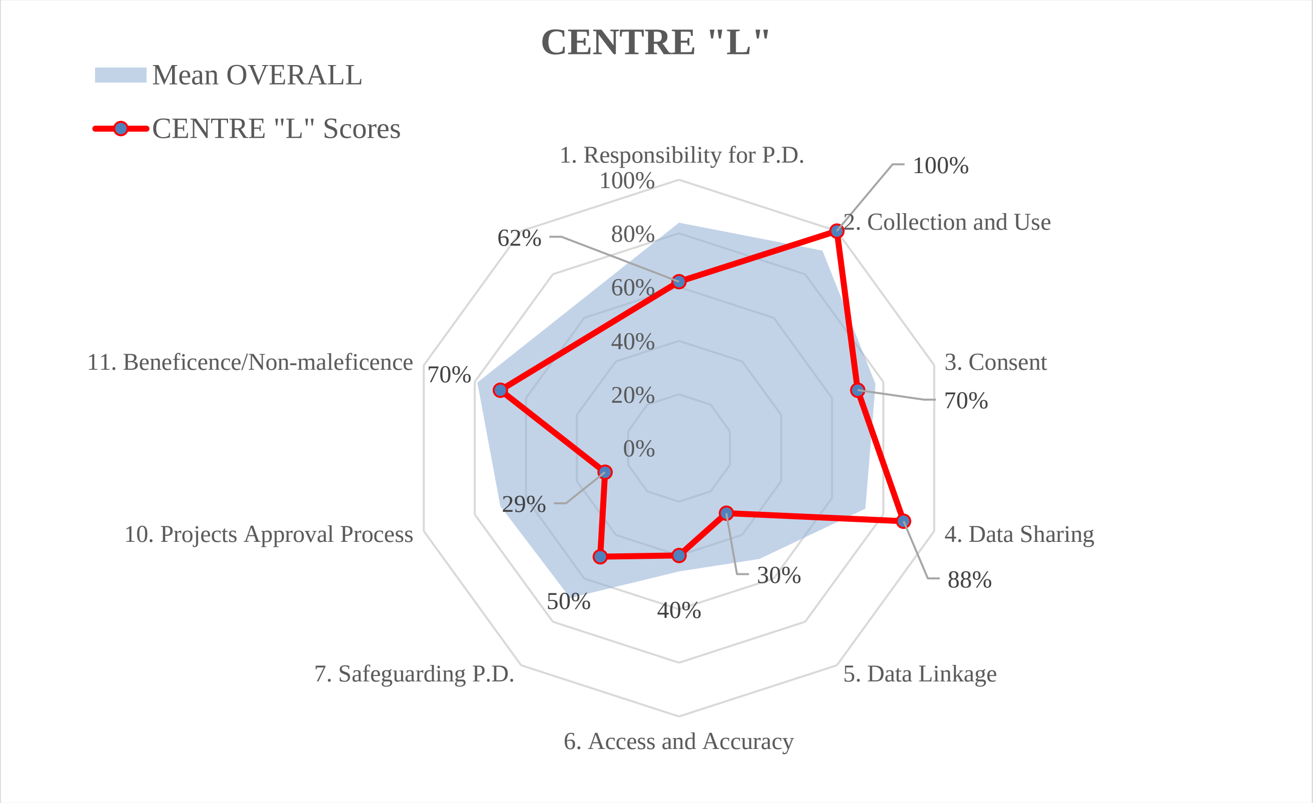

CENTRE "G"
Mean OVERALL
CENTRE "G" Scores
1. Responsibility for P.D.
2. Collection and Use
3. Consent
4. Data Sharing
5. Data Linkage
6. Access and Accuracy
7. Safeguarding P.D.
8. Anonymisation
9. Openness
10. Projects Approval Process
11. Beneficence/Non-maleficence
100%
80%
60%
40%
20%
0%
92%
90%
70%
63%
40%
50%
40%
11%
0%
29%
50%

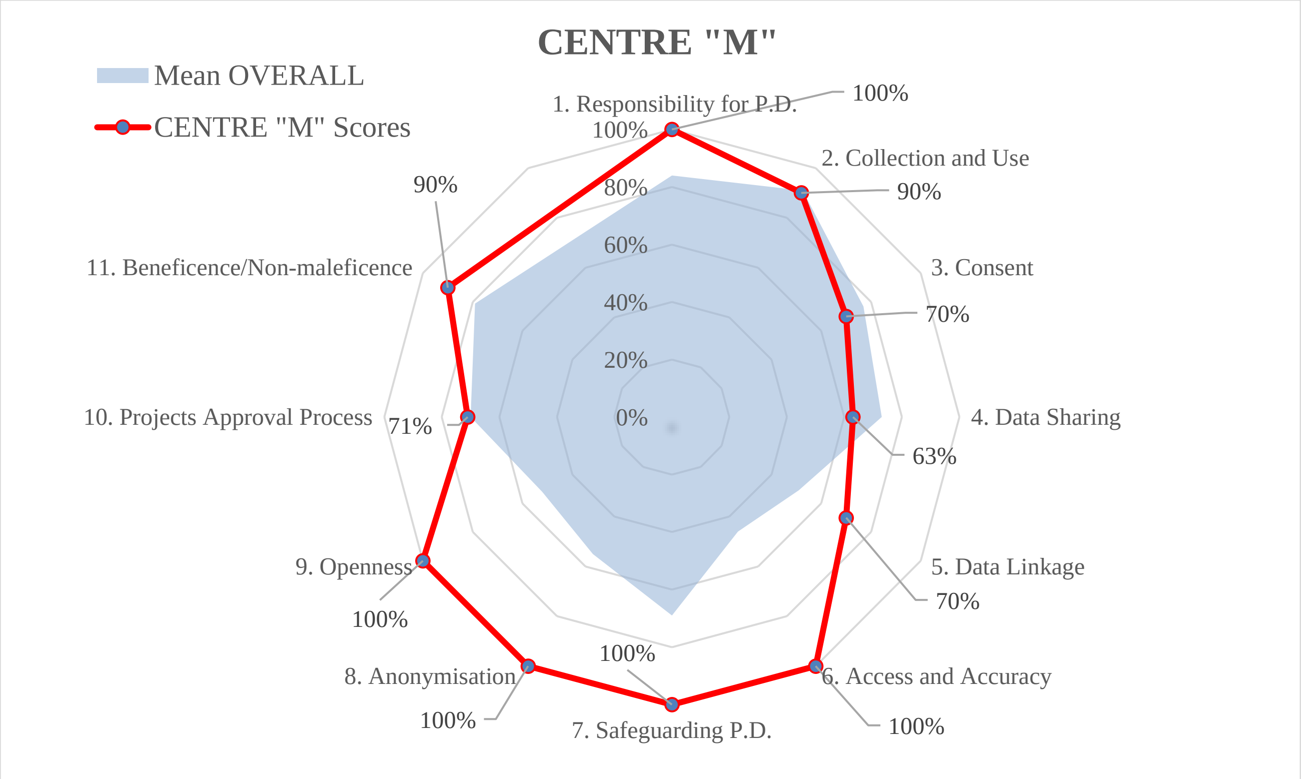

CENTRE "H"
Mean OVERALL
CENTRE "G" Scores
1. Responsibility for P.D.
2. Collection and Use
3. Consent
4. Data Sharing
5. Data Linkage
6. Access and Accuracy
7. Safeguarding P.D.
8. Anonymisation
9. Openness
10. Projects Approval Process
11. Beneficence/Non-maleficence
100%
80%
60%
40%
20%
0%
69%
90%
70%
100%
50%
30%
70%
33%
67%
100%
79%

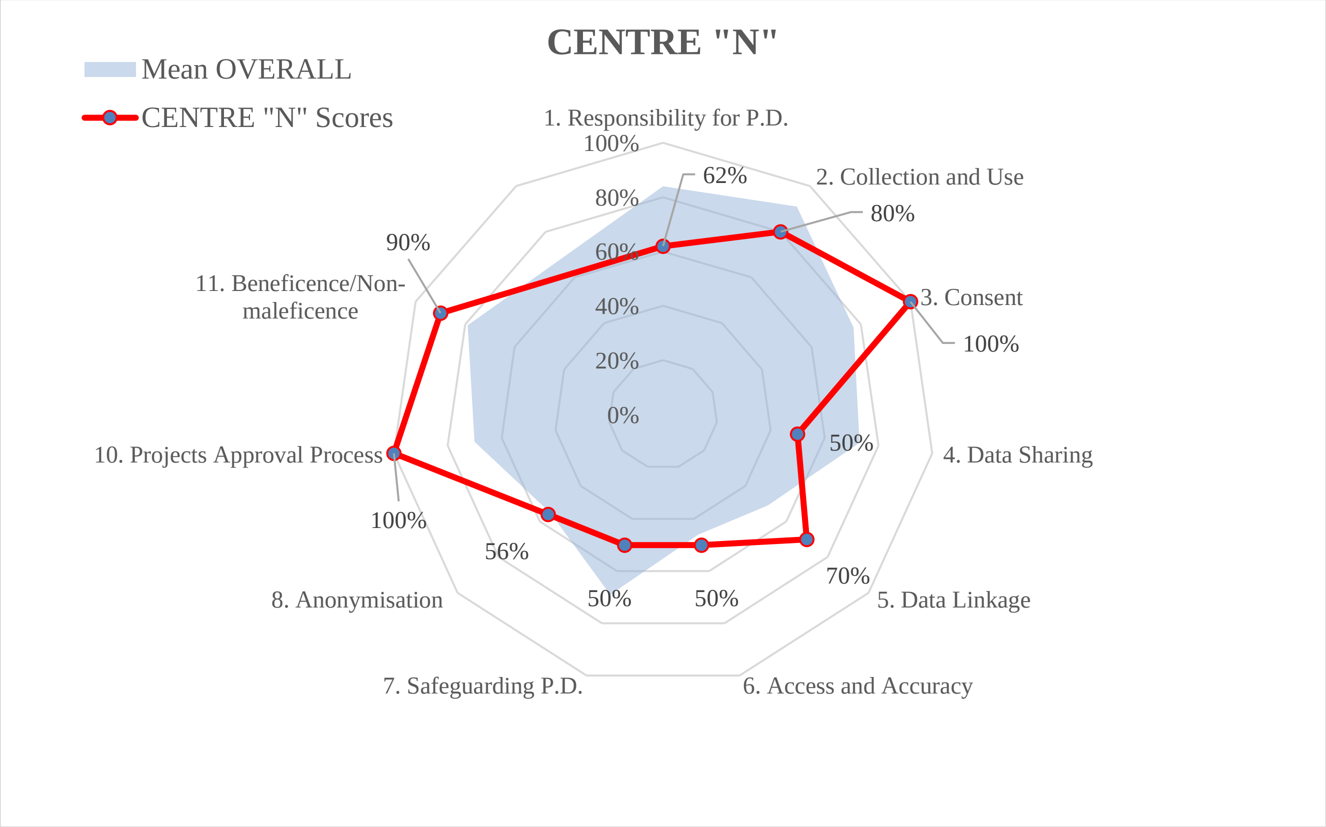

CENTRE "I"
Mean OVERALL
CENTRE "I" Scores
1. Responsibility for P.D.
2. Collection and Use
3. Consent
4. Data Sharing
5. Data Linkage
7. Safeguarding P.D.
8. Anonymisation
10. Projects Approval Process
11. Beneficence/Non-maleficence
100%
80%
60%
40%
20%
0%
100%
90%
70%
75%
80%
70%
89%
71%
80%

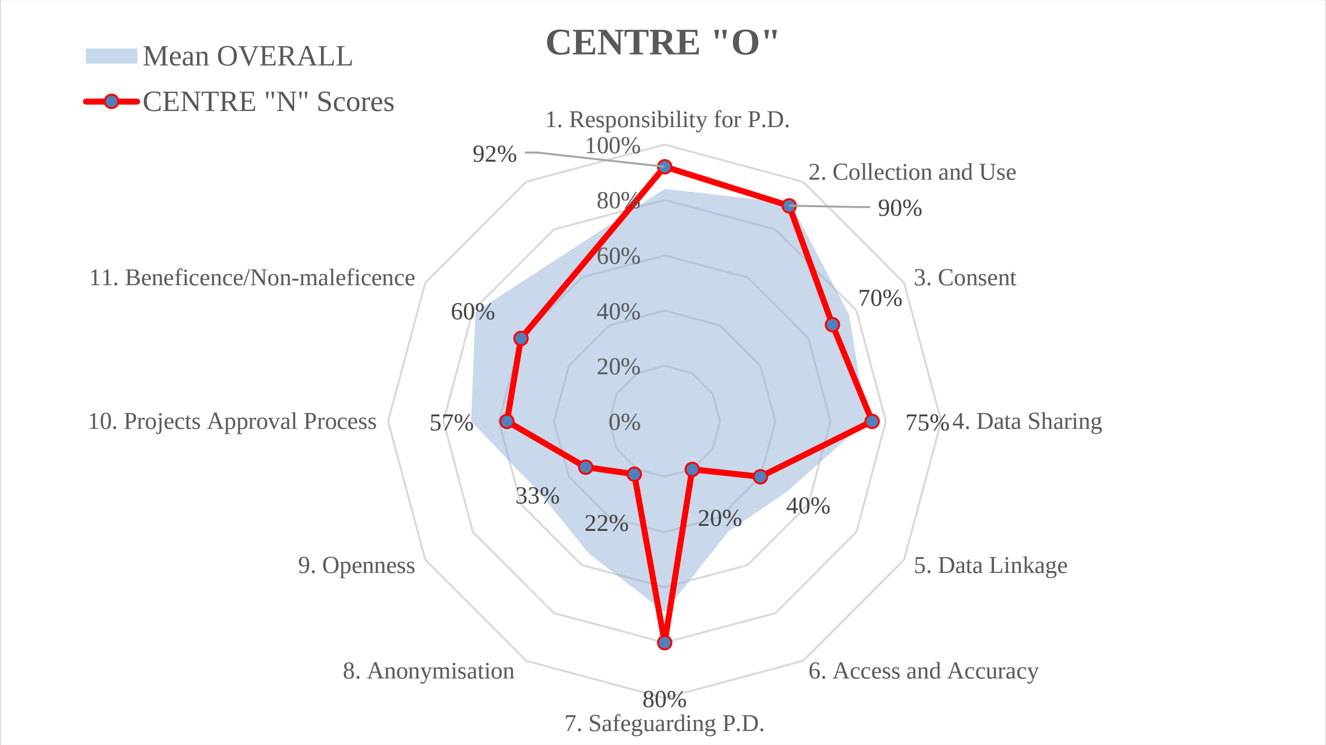

CENTRE "J"
Mean OVERALL
CENTRE "J" Scores
1. Responsibility for P.D.
2. Collection and Use
3. Consent
4. Data Sharing
5. Data Linkage
7. Safeguarding P.D.
9. Openness
10. Projects Approval Process
11. Beneficence/Non-maleficence
100%
80%
60%
40%
20%
0%
62%
100%
80%
50%
30%
60%
33%
14%
90%


CENTRE "K"
Mean OVERALL
CENTRE "K" Scores
1. Responsibility for P.D.
2. Collection and Use
3. Consent
4. Data Sharing
5. Data Linkage
6. Access and Accuracy
7. Safeguarding P.D.
9. Openness
10. Projects Approval Process
11. Beneficence/Non-maleficence
100%
80%
60%
40%
20%
0%
92%
90%
70%
88%
60%
0%
70%
67%
100%
80%


CENTRE "L"
Mean OVERALL
CENTRE "L" Scores
1. Responsibility for P.D.
2. Collection and Use
3. Consent
4. Data Sharing
5. Data Linkage
6. Access and Accuracy
7. Safeguarding P.D.
10. Projects Approval Process
11. Beneficence/Non-maleficence
100%
80%
60%
40%
20%
0%
62%
100%
70%
88%
30%
40%
50%
29%
70%


CENTRE "M"
Mean OVERALL
CENTRE "M" Scores
1. Responsibility for P.D.
2. Collection and Use
3. Consent
4. Data Sharing
5. Data Linkage
6. Access and Accuracy
7. Safeguarding P.D.
8. Anonymisation
9. Openness
10. Projects Approval Process
11. Beneficence/Non-maleficence
100%
80%
60%
40%
20%
0%
100%
90%
70%
63%
70%
100%
100%
100%
100%
71%
90%


CENTRE "N"
Mean OVERALL
CENTRE "N" Scores
1. Responsibility for P.D.
2. Collection and Use
3. Consent
4. Data Sharing
5. Data Linkage
6. Access and Accuracy
7. Safeguarding P.D.
8. Anonymisation
10. Projects Approval Process
11. Beneficence/Non-maleficence
100%
80%
60%
40%
20%
0%
62%
80%
100%
50%
70%
50%
50%
56%
100%
90%


CENTRE "O"
Mean OVERALL
CENTRE "N" Scores
1. Responsibility for P.D.
2. Collection and Use
3. Consent
4. Data Sharing
5. Data Linkage
6. Access and Accuracy
7. Safeguarding P.D.
8. Anonymisation
9. Openness
10. Projects Approval Process
11. Beneficence/Non-maleficence
100%
80%
60%
40%
20%
0%
92%
90%
70%
75%
40%
20%
80%
22%
33%
57%
60%

5.2 BRIDGE-Health Privacy and Ethics Analysis

The survey conducted in the BRIDGE-Health project through the PEIPA questionnaire has allowed an objective assessment of the level of adherence to the European Data Protection Regulation and compliance to privacy and ethics principles/guidelines/best practices of health registries/databases/information systems involved in the study.

Scope of the BRIDGE-Health PEIPA was to answer the following questions:

- How heterogeneous is the implementation of privacy and ethics requirements/principles/best practices among participating centres?
- What are the key areas of concern on which advice and guidance is most needed?
- How can the consistency of privacy and ethics requirements set by EU and international legislation/guidelines be managed and improved by participating centres?

The sample of centres included in the survey, although not representative of the state of the art across all Europe, offers a substantial overview of the topic across 9 EU countries. The sample is composed of centres from different European countries that are members of 3 consortia, namely ECHO, EUROHOPE and EUBIROD. Each consortium is composed of a different share of countries.

ECHO centres cover the following geographical areas:

- Denmark (CHOPES) (N.=1)
- Slovenia (N.=1)
- Spain (N.=1)
- Austria (N.=1)

EUROHOPE centres cover the following geographical areas:

- Finland (N.=1)
- Hungary (N.=1)
- Norway (N.=1)
- Spain (N.=1)
- Denmark (N.=1)

EUBIROD centres cover the following geographical areas:

- Croatia (N.=2)
- Norway (N.=1)
- Romania (N.=1)
- Poland (N.=1)
- Slovenia (N.=1)

The PEIPA questionnaire has been used to collect information on all foreseeable privacy and ethics issues that might be incurred in the management of BRIDGE-Health registries/databases/information systems.

The Privacy and Ethics Impact and Performance Assessment (PEIPA) performed in the BRIDGE-Health project involves the adoption of a new metrics, initially developed in the context of the EUBIROD project, which allows a quali-quantitative analysis of the PEIPA questionnaires responses. The analysis could be automated through an IT platform, including a web version of the questionnaire.

The analysis has been facilitated by the definition of a scoring system. A scoring table has been developed for each factor, based on the assumption that scores for that particular issue can provide a linear measure of the level of privacy protection and ethics compliance of the procedures implemented in participating centres, according to the relevant legislation/guidelines/principles.

Descriptive analysis has been facilitated by recoding original responses (YES/NO/NA) as to assign marks in terms of compliance/not compliance to privacy and ethics principles/norms (e.g. YES=1).

The proposed metrics has been validated by the ad hoc Panel of Experts, who reviewed both the PEIPA questionnaire and the scoring system and contributed to the finalization of the PEIPA Results Report herein included as section 5.

Hence, the proposed metrics can be considered a validated system aimed to measure the degree of heterogeneity in the implementation of privacy and ethics principles/norms and the level of privacy protection and ethics compliance across Europe.

Responses to single questions highlight the following:

- Registries/databases/information systems normally implement privacy by design and privacy by the default (93.4% of cases) measures and conduct privacy impact assessments (73.4% of cases); while accountability is documented only in the 66.7 % of cases.
- The use of data for secondary purposes is widely allowed for approved research (93.4% of cases); while it is used to report on healthcare quality only in the 66.7% of cases. To this aim, data is always de-identified before it is used for secondary purposes.
- Consent is not required to collect data in the registries/databases/information systems in the majority of cases (60%). In all cases where consent is not required, it is waived by law. However, the possibility for the data subject to opt out is minimal (11% of cases); which highlight a privacy concern that needs to be addressed.
- On the other end, where consent is required to collect data in the registries/databases/information systems, it is normally obtained from the individual (83.4% of cases) and the data subject can refuse/withdraw consent (66.8% of cases).
- Data controllers are allowed to share de-identified data with public authorities/academic/no profit research organizations in most cases (80%); while the cross-border data flow decreases to 66.7% of cases.

- Data linkage is performed by the 80% of the involved registries/databases/information systems; however, in some cases the way data linkage is performed pose concerns relative to the use of direct identifiers.
- The anonymisation process is normally reported as compliant with international standards (81.8% of cases). However, anonymisation techniques implemented do not coincide with those suggested by EU opinions/guidelines (i.e. Randomization and/or Generalization or a combination of the two).

The analysis of individual factors shows that the major areas of concern (median, range) are:

- Data linkage (median: 45%; range: 30-80%)
- Access and accuracy of personal data (median: 50%; range: 0-100%)
- Anonymisation (median: 56%; range: 11-100%)

Factors showing on average a high variability include the following:

- Safeguarding personal data (range: 30-100%)
- Openness (range: 0-100%)
- Transparent health research projects approval process (range: 14-100%)
- Data sharing (range: 50-100%)
- Beneficence/non maleficence principles in health research project approval processes (range: 50-100 %)

The high variability of scores detected in the BRIDGE-Health sample for most of the factors analysed reveals a heterogeneous implementation of privacy and ethics principles across involved centres; highlighting the need to implement corrective measures at both EU and national levels.

The range of overall scores achieved by each BRIDGE-Health registry/database/information system (i.e. sum of the scores, expressed as a percentage of maximum score, obtained in each factor) spans from 49% to 91% (mean: 70%) with a median of 69% and 20% of the sample falling above 80% of the maximum performance. The 53.3% of the sample achieved an overall score between 61% and 79% (“fair” privacy and ethics performance).

The BRIDGE-Health survey has produced a detailed description of how personal information is handled in 15 registries/databases/information systems across Europe, allowing an identification of the key areas of privacy and ethics concern in health data management and an overview of the variability of approaches at European level.

Privacy performance has been measured against both absolute and mean values obtained for the whole sample. The rationale for providing both values is that, theoretically, a perfect adherence to all privacy and ethics principles and requirements is obviously desirable. However, providing mean values of BRIDGE-Health centres allows comparing the performance of individual centres against values obtained in comparable practical settings. Thus, it provides fruitful information on the extent to which privacy and ethics norms/requirements have been practically implemented across Europe.

The findings of this survey could be used to develop targeted actions at both European and National levels. While the EU should provide suitable guidelines to Member States aimed to increase the level of adherence to privacy and ethics principles in the highlighted areas of concern, Member States should ensure that individual users apply all regulations/guidelines/best practices in line with principles and norms internationally agreed, without jeopardizing health goals.

Legislation should therefore recognize the importance of data processing operations that are crucial to improve health and health research. However, it is also fundamental that the ethical values enshrined in EU and international legislation are fully respected across Europe.

The PEIPA tool could be used as a means to foster privacy enhancing registries/databases/information systems and to reconcile the conflicting interests of health research and privacy.

The PEIPA tool realized in the BRIDGE-Health project could be used as a general model of collaborative privacy and ethics performance evaluation, fostering the creation of privacy enhancing registries/databases/information systems.

The PEIPA tool represents an innovative methodology aimed, among the others, to feed information back to individual centres. Each survey respondent can be directly and anonymously informed of its own areas of concern (factors performance) in terms of deviation from privacy/ethics requirements and best practices. Single centres can then easily enforce appropriate safeguards for those data processing operations that pose privacy risks. For instance, data linkage could be safely performed using pseudonymous instead of direct identifier, or through trusted third parties that would guarantee the respect of privacy norms and best practices.

The tool can also improve the quality of information contained in registries/databases/information systems. For instance, the low score obtained by the sample in the factor "access and accuracy of personal data" may also indicate issues of data quality that can ultimately hamper the research validity of the information included in the registries/databases/information systems. Once revealed, the issue can be easily improved/resolved through the adoption of corrective measures.

The PEIPA tool can be finally used to provide benchmarks for privacy, ethics and best practices compliance: the combination of the scoring tables with the relative sections of the questionnaire provide the "gold standard" measures and practices for the processing of health related data in registries/information systems/databases, from which suitable guidelines could be easily drawn out.

6. Conclusions

The validated model of Privacy and Ethics Impact and Performance Assessment developed in BRIDGE-Health (PEIPA) can help data controllers/data protection officers of registries/databases/information systems to easily accomplish privacy and ethics requirements by identifying the main areas of concern, including those that can impact on the quality of information, and directly implement corrective measures at the level of the individual centre.

The model fosters collaboration, rather than competition on privacy performance, in order to generate both privacy and ethics enhancing registries/databases/information systems and quality improvement loops that can increase data accuracy and completeness.

On the other end, targeted actions at both European and National levels should be put in place to foster a harmonized implementation of privacy and ethics principles and requirements both across Member Stated and within countries. To this aim, the tool could provide benchmarks for privacy, ethics and best practices compliance and foster the development of target guidelines at both European and national level.

A concerted action at both the legislative level and point of care provision is needed to achieve a right balance between privacy and health research.

Appendix 1: PEIPA Questionnaire

Introduction to PEIPA Questionnaire

How to fill in the Questionnaire

The PEIPA questionnaire provides a series of questions aimed to assess the adherence to EU, OECD and International privacy and ethics principles, regulations guidelines and best practices.

The questionnaire is a core element of the Privacy and Ethics Impact and Performance Assessment, (PEIPA), a methodology that draws from the EUBIROD Privacy Impact Assessment(1,2).

The questionnaire is addressed to data controllers and/or data protection officers and/or chief executive officers eventually responsible for data processing in the ECHO, EUROHOPE and EUBIROD consortia.

The questionnaire is composed of 11 sections (factors), each containing a specific number of questions (sub-factors).

Results from filled in questionnaires will be analysed through a mixed quali-quantitative analysis.

Results will be made available to participants and to the wider community in de-identified and/or aggregated format, also via the Final Report.

Respondents are required to provide YES/NO responses to a series of questions, which are divided into 11 sections. "N/A" (not applicable) option is also available for cases where single questions or one or more entire sections are not applicable to the respondent. The "Provide Details" column should be used to explain responses or to provide specific references. Privacy is herein intended to be a broader concept than legal compliance; hence, it was recommended to provide comments and details in accurate and comprehensive manner.

Definitions

Personal data means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person;

De-identification means the processing of personal data in such a manner that data cannot identify an individual directly or indirectly. De-identification requires the removal of name and exact address; and can also involve the removal of any other detail or combination of details that might support identification.

Anonymous data means data which does not relate to an identified or identifiable natural person ('data subject') or personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable using any reasonable means. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

Data controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the data controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller;

Recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

Third party means a natural or legal person, public authority, agency or body other than the data subject, data controller, processor and persons who, under the direct authority of the data controller or processor, are authorised to process personal data;

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

Supervisory Authority means an independent public authority which is established by a Member State pursuant to Article 51 of the DPR (2016);

Cross-border processing means either:

- processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a data controller or processor in the Union where the data controller or processor is established in more than one Member State; or
- processing of personal data which takes place in the context of the activities of a single establishment of a data controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

Record linkage refers to a merging that brings together identifiable records from two or more sources of data with the object of consolidating facts concerning an individual or an event that are not available in any separate record (Handbook of Vital Statistics Systems and Methods, Vol. 1: Legal, Organizational and Technical Aspects, United Nations Studies in Methods, Glossary, Series F, No. 35, United Nations, New York, 1991.) An example would be linking patient records in a hospital database to any death records for the same persons in a mortality registry in order to identify patients who died following treatment. Deterministic record linkage, often referred to as exact matching, occurs when a unique identifier or set of identifiers is used to merge two or more sources of data. In health linkages, the identifier used is often a unique patient identifying number or UPI. Probabilistic record linkage occurs when a set of possible matches among the data sources to be linked are identified. For example, identifying information such as names, dates of birth, and postal codes, may be used to assess potential matches. Then statistics are calculated to assign weights describing the likelihood the records match. A combined score represents the probability that the records refer to the same entity. Often there is one threshold above which a pair is considered a match, and another threshold below which it is considered not to be a match. This technique is used when an exact match between records across databases is not possible, or when data capture errors have caused deterministic matches to fail.

Sometimes deterministic matching does not provide a perfect match (e.g. matching on a unique local system ID which might be repeated on other local systems). In these circumstances mixed probabilistic and deterministic methods can be used (de Lusignan S, Navarro R, Chan T, Parry G, Dent-Brown K, Kendrick T. Detecting referral and selection bias by the anonymous linkage of

practice, hospital and clinic data using Secure and Private Record Linkage (SAPREL): case study from the evaluation of the Improved Access to Psychological Therapy (IAPT) service. BMC Med Inform Decis Mak. 2011 Oct 13;11:61. doi: 10.1186/1472-6947-11-61).

PEIPA Questionnaire

Respondent & Organization Details

Please fill in the Respondent and Organization details table below

First Name	
Last Name	
Email address	
Telephone Number	
Institution/organization/ Centre name	
Institution/organization/ Centre address, including country	
Respondent Role: please indicate your role in the institution (e.g. data controller, data protection officer, chief executive officer)	
Consortia: Please indicate what consortia your institution belongs to (e.g. ECHO, EUROHOPE; EUBIROD)	

1. Responsibility for Personal Data

Questions For Analysis	Yes	No	N/A	Provide Details
1.1 Has the data controller of the registry/database/information system been nominated/established/identified?				
1.2 Is there just one data controller for the registry/database/information system?				
1.3 Are there several data controllers responsible for different data processing occurring in the registry/database/information system?				
1.4 If there are several data controllers, have all data controllers been clearly identified?				
1.5 Has the data controller determined the set of purposes and means of the various processing occurring in the registry/database/information system?				
1.6 Has the data controller implemented a data protection policy for the registry/database/information system aimed to ensuring that personal data are: • processed lawfully, fairly and in a transparent manner • collected for specified, explicit and legitimate purposes • adequate, relevant an limited to what is necessary for the purpose of the processing • accurate and up to date • kept in identifiable form for no longer than necessary to the aims of the processing • Kept secure and confidential?				
1.7 Has the data controller implemented appropriate technical and organisational measures embedding privacy protective technologies (e. g. pseudonymisation, encryption) in the registry/database/information system (privacy by design)?				
1.8 Has the data controller implemented appropriate technical and organisational measures to ensure, by default, adherence to privacy principles (e.g. data minimisation principle) in the registry/database/information system?				
1.9. Does the data controller conduct privacy/data protection impact assessments, when processing involve a high risk for privacy; e.g. processing on a large scale of health related data?				
1.10 Has the data controller put in place measures to ensure that it is able to demonstrate (e.g. through audits/checks) and document the effectiveness of the above mechanisms (accountability)?				

1.11 Has the data controller nominated the processor/processors and provided them with documented instructions for the processing of personal data in the registry/database/information system?				
1.12 If processors are nominated, does the data controller have an agreement/contract in place with them that sets forth the subject matter and duration of the processing, the parties obligation and rights, the share of privacy/data protection responsibilities, etc.?				
1.13 If third parties processors are involved, have they been authorized in writing by the data controller and bound to the same obligations of the data controller and processor?				

2: Collection & Use of Personal Data

Questions For Analysis	Yes	No	N/A	Provide Details
2.1 Do you collect personal data in the registry/database/information system? If you do not collect personal data, please fill this section with all N/A and proceed to next section.				
2.2 Do you have a legal base (authorized by national/regional law, regulation, Supervisory Authority) to collect personal data in the registry/database/information system?				
2.3 Is all the personal data collected necessary to the registry/database/information system; i.e. limited to what is necessary in relation to purposes of the registry/database/information system, as set out by the data controller?				
2.4 Are data controllers of the registry/database/information system allowed to use data for secondary purposes; e.g. approved health research and statistics?				
2.5 If yes, are the secondary uses compatible with the purposes for which data were previously collected?*				
2.6 Is this data used to regularly report on health care quality or health system performance?				
2.7 If personal data is to be used or disclosed for a secondary purpose not previously identified, is consent required?				
2.8 If consent is not required for secondary purpose use or disclosure, is there authority for the use or disclosure; e.g. processing for research or public health purposes is authorized by law, regulation, Data Protection Authority?				
2.9 Is data de-identified and/or pseudonymised before it is used for any secondary purpose, including data linkage?				
2.10 Is information anonymised when used for planning, management and/or evaluation purposes?				

* The secondary use of personal data for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes are considered, in principle, compatible with the initial purposes of the data collection [Art 5(1,b) of Regulation (EU) 2016/679 of the Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)].

3. Consent

Questions For Analysis	Yes	No	N/A	Provide Details
3.1 Is consent required to collect and process personal health data in the registry/database/information system? If consent is required, please respond N/A to questions 3.2 and 3.3 and proceed to questions 3.4, 3.5, 3.6, 3.7, 3.8, 3.9 and 3.10.				
3.2 If consent is not required, is it waived by law? If consent is not required, please respond only to questions 3.2 and 3.3and respond N/A to questions 3.4, 3.5, 3.6, 3.7, 3.8, 3.9 and 3.10.				
3.3 If consent is not required, can the data subject opt-out? If the data subject cannot opt out, please explain the reasons in the provide details column.				
3.4 If consent is required, is it obtained directly from the individual?				
3.5 If consent is required, are you able to demonstrate that consent has been freely given, informed and unambiguous?				
3.6 If consent is required, is it given either for one or more specified purposes?				
3.7 If consent is required, can the data subject refuse to consent to the collection or use of personal data for a secondary purpose, unless required by law?				
3.8 If consent is required, can the data subject withdraw his/her consent at any time?				
3.9 If consent is required, is a broad consent to further uses of registry/database/information system data and/or data linkage allowed for approved health studies and research?				
3.10 If consent is required, is a broad consent to any further (non-health related research) uses of health data and/or data linkage allowed?				

4. Data Sharing

Questions For Analysis	Yes	No	N/A	Provide Details
4.1 Are data controllers allowed to share readily identifiable health data for statistics or research with public authorities and/or academic or private organisations for non-commercial purposes?				
4.2 Are data controllers allowed to share de-identified or pseudonymised health data with another public authority and/or academic or private organisations for non-commercial purposes?				
4.3 Are data controllers allowed to share readily identifiable health data for statistics or research with foreign public authorities and or academic or private organisations for non-commercial purposes (cross-border data flow)?				
4.4 Are data controllers allowed to share de-identified or pseudonymised health data for statistics and research with another foreign public authority and or academic or private organisations for non-commercial purposes?				
4.5 Do you have a standard data sharing agreement for disclosing data (or multiple standard ones for different types of data requestors)?				
4.6 Does your data sharing agreement require certain privacy/security practices at the data recipient's site?				
4.7 Does your data sharing agreement state what penalties would occur if privacy/security practices are not respected (i.e. data breach)?				
4.8 Does your data sharing agreement stipulate procedures/restrictions regarding the publication of data (indirect disclosure) and data retention?				

5. Data Linkage

Questions For Analysis	Yes	No	N/A	Provide Details
5.1 Are you allowed to perform data linkages? If you are not allowed or you do not perform data linkage, please fill in this section with all N/A and proceed to next section				
5.2 Is record linkage performed using the registry/database/information system records, without applying measures to ensure privacy/data protection (e.g. pseudonymisation, de-identification)?				
5.3 Are unique personal identifiers, such as a social insurance number, used for the purposes of linking across multiple databases (deterministic record linkage) without applying measures to ensure privacy/data protection (e.g. pseudonymisation, de-identification?				
5.4 Do you use identifying attributes (such as name, sex, birth date, address) to link multiple sources (*probabilistic record linkage)?*				
5.5 Do you apply standard practices for deleting direct identifiers (such as names and patient numbers) for the performance of data linkages?				
5.6 Do you apply standard practices for deleting direct identifiers (such as names and patient numbers) after the data linkage has been finalized?				
5.7 Do you apply practices for creating pseudonyms from direct identifiers?				
5.8 Is the de-identification and/or pseudonymisation methodology documented?				
5.9 Do you use a standard process for the assessment of the risk of data re-identification?				
5.10 Do you use standard practices for the treatment of attributes that pose a re-identification risk (such as rare diseases, exact dates, locations, or ethnic origins)?				

6. Access and Accuracy of Personal data

Questions For Analysis	Yes	No	N/A	Provide Details
6.1 Is the registry/database/information system designed to ensure that an individual can have access to his/her personal information? If the registry/database/information system does not collect or process personal data, please fill in this section with all N/A and proceed to next section.				
6.2 Is the registry/database/information system designed to ensure that an individual can request the rectification or erasure of personal information?				
6.3 Is the registry/database/information system designed to ensure that an individual can request the restriction of processing of personal data?				
6.4 Is the registry/database/information system designed to ensure that an individual can object to the processing of personal data?				
6.5 Does the data controller provide the data subject access to personal data and information to the data subject (e.g. purpose of the processing, categories of data, recipients, storage duration)?				
6.6 Is the data subject informed of his/her right to lodge a complaint?				
6.7 If personal information is not collected from the data subject, do the data controllers/processors provide any available information to the data subject as to their source (e.g. the identity of the controller, the purpose of the processing, the category of data, the recipients, the existence of the right to request from the controller access to and rectification or erasure of personal data, etc. unless it involves a disproportionate effort)?				
6.8 Does the record of personal information indicate the date of last information update and the source of information used to make changes?				
6.9 Is there a clearly defined process by which an individual may access, assess and discuss or dispute the accuracy of the record?				
6.10 Is there a record kept with respect of requests for a review of errors or omissions & corrections or decisions not to correct?				

7. Safeguarding Personal Data

Questions For Analysis	Yes	No	N/A	Provide Details
7.1 Are security measures compliant with international standard according to the state of the art? E.g. Any of the following ones: ISO 27001:2013, a standard for information security management; ISO 27002:2013, a catalogue of information security controls; ISO 27005:2011, a standard for information security risk management? * (Please note the list is not exhaustive. Please respond "YES" and provide details if comparable standards are complied with?)				
7.2 Is compliance with international standards certified by accredited registration bodies (e.g. assessment and registration bodies, certification/ registration bodies or registrars)?*				
7.3 Have security procedures for the collection, transmission, storage and disposal of personal information, and access to it, been documented?				
7.4 Are there controls in place for any process to grant authorization to modify (add, change or delete) personal information from records?				
7.5 Are user accounts, access rights and security authorizations controlled by a system or record management process?				
7.6 Are security/technical and organizational measures commensurate with the sensitivity of the information recorded?				
7.7 Are employees who have permanent or regular access to personal data appropriately trained in the requirements for protecting personal information and are they aware of the relevant policies regarding breaches of security, integrity or confidentiality?				
7.8Are there contingency plans and documented procedures in place to identify and respond to security breaches or disclosures of personal information in error?				
7.9 Are there documented procedures in place to communicate/notify security violations to the data subject, law enforcement authorities and relevant program managers when there is a risk to the rights and freedom of data subjects?				
7.10 Is there a plan for quality assurance and audit programs to assess the ongoing state of the safeguards applicable to the system?				

* "ISO/IEC 27001 provides normative requirements for the development and operation of an ISMS, including a set of controls for the control and mitigation of the risks associated with the information assets which the organization seeks to protect by operating its ISMS. Organizations operating an ISMS may have its conformity audited and certified. In some countries, the bodies that audit and certify conformity to specified standards are called "certification bodies", while in others they are commonly referred to as "registration bodies", "assessment and registration bodies", "certification/ registration bodies", and sometimes "registrars".

8. Anonymisation Process [(6)]

Questions For Analysis	Yes	No	N/A	Provide Details
8.1When anonymisation is required for the further processing of personal data contained in the registry/database/information system, does your centre/institution has to apply a standard anonymisation procedure?				
8.2 If yes, is the applied procedure compliant with international technical standards and continuously updated according to the state of the art?				
8.3 If yes, is the anonymisation process performed in compliance with the Data Protection Principles; for instance, performed confidentially, providing information to patients about the processing operation, applying security mechanisms for data storage and retention, etc.?				
8.4 Is the anonymisation process documented?				
8.5 Are Anonymisation techniques implemented aimed to minimize all of the following risks: • Singling out, which corresponds to the possibility to isolate some or all records which identify an individual in the dataset; • Linkability, which is the ability to link, at least, two records concerning the same data subject or a group of data subjects (either in the same database or in two different databases). • Inference, which is the possibility to deduce, with significant probability, the value of an attribute from the values of a set of other attributes				
8.6 Are Randomization techniques (e.g Noise addition, Permutation, Differential privacy) used in the anonymisation process?				
8.7 Are Generalization techniques (e.g. Aggregation and K-anonymity, L-diversity/T-closeness) used in the anonymisation process?				
8.8 Is a combination of Randomization and Generalization techniques used in the anonymisation process? If you answered yes to 8.8, please check you answered yes to 8.6 and 8.7 as well.				
8.9 Are anonymisation techniques/mix of techniques being implemented disclosed, especially when it is envisaged the release of the anonymised dataset?				

9. Openness, Transparency & Public Engagement

Questions For Analysis	Yes	No	N/A	Provide Details
9.1 Is the public consulted and/or informed about the collection and processing of personal health related data in the registry/database/information system? If you do not collect and/or process personal data, please fill in this section with all N/A and proceed to next section.				
9.2 Is there a communication plan/strategy to explain to the public how personal information will be collected, managed and protected? If NOT, please respond N/A to 9.3, 9.4,9.5.				
9.3 Does the communication plan/strategy include information on the benefits of the processing, the risks of the processing and risk mitigations strategies?				
9.4 Does the communication plan/strategy include public information, such as a website, that describes the content of datasets and dataset data controllers and processors?				
9.5 Does the communication plan/strategy include public information, such as a website, that describes applications for approval of the processing of health datasets, including dataset linkages, as well as approval decisions?				
9.6 Is a certification/accreditation process for the processing of health data for research and statistics implemented?				

10. Transparent Health Research Projects Approval Process

Questions For Analysis	Yes	No	N/A	Provide Details
10.1 When research projects are carried out using health related data contained in the registry/database/information system, do you have a national/regional/local project approval bodies that authorize the research?				
10.2 Are project approval bodies multidisciplinary; e.g. include relevant stakeholders, such as legal experts, privacy experts, statistical experts, patients and researchers that are also third parties, with no stake in an approval process?				
10.3 Are data controllers involved (or consulted upon) in the project approval process?				
10.4 Are approval bodies publicly identified, including body's role and membership?				
10.5 Are the criteria that the body follows for project approval publicly identified/accessible, including timeliness of approval decisions?				
10.6 Are approval bodies accountable for the timeliness and quality of their services?				
10.7 Are complaint procedures envisaged to appeal against approval bodies' decisions?				

11. Beneficence/Non-maleficence Principles in Health Research Project Approval Processes

Questions For Analysis	Yes	No	N/A	Provide Details
11.1 Do you conduct research projects using health related data contained in the registry/database/information system? If NOT, please respond N/A to all other questions of this last section.				
11.2 If yes, have they comply with protocols/guidelines/code of conduct that ensure that rights and dignity of patients are considered and respected?				
11.3 Are the burdens and potential harms of the research project identified, considered, taken into account and documented?				
11.4 Are risk assessments for single techniques and for the proposal as whole performed?				
11.5 Are there standard procedures to assess that burdens and potential harms, if any, are justified in the light of the potential benefit to participants and/or to society?				
11.6 Are the potential benefits of the research projects as a whole identified?				
11.7 Are project results aimed to improve any of the followings: • health outcomes, • treatments, • quality of health care, • efficiency, cost or affordability of health care, • the management or governance of the health sector, • patients' health care experiences?				
11.8 Are there standard procedures to assess that the selection of participants (recruitment criteria) in the research projects is fair and appropriate?				
11.9 Are the potential long term consequences of the research project considered, addressed and documented?				
11.10 Is the potential for misuse (e.g. malevolent/criminal/terrorist abuse) considered and, if any addressed and documented?				

Appendix 2: Scoring Tables

Table 1: Responsibility for Personal Data

Questions For Analysis	Yes	No	N/A
1.1	1	0	
1.2	1	1	
1.3	1	1	
1.4	1	0	1
1.5	1	0	
1.6	1	0	
1.7	1	0	
1.8	1	0	
1.9	1	0	
1.10	1	0	
1.11	1	0	
1.12	1	0	
1.13	1	0	1

(**Max Score = 13)**

Table 2: Collection & Use of Personal Data

Questions For Analysis	Yes	No	N/A
2.1	1	0	1
2.2	1	0	1
2.3	1	0	**1**
2.4	1	0	
2.5	1	0	
2.6	1	0	
2.7	1	0	1
2.8	1	0	1
2.9	1	0	
2.10	1	0	

(Max Score = 10)

Table 3: Consent

Questions For Analysis	Yes	No	N/A
3.1	1	0	
3.2	7	0	**1**
3.3	3	0	**1**
3.4	1	0	
3.5	1	0	
3.6	1	0	
3.7	1	0	
3.8	1	0	
3.9	1	0	
3.10	0	1	

(Max Score = 10)

If 3.1 =YES, 3.2 and 3.3 = N/A; then for 3.2 and 3.3 N/A= 1

If 3.1 = NO, 3.2 and 3.3 = N/A; then for 3.2 and 3.3 N/A= 0

Table 4: Data Sharing

Questions For Analysis	Yes	No	N/A
4.1	0	1	
4.2	1	0	
4.3	0	1	
4.4	1	0	
4.5	1	0	
4.6	1	0	
4.7	1	0	
4.8	1	0	

(Max Score = 8)

Table 5. Data Linkage

Questions For Analysis	Yes	No	N/A
5.1	1	1	
5.2	0	1	
5.3	0	1	
5.4	0	1	
5.5 *	1	0	
5.6	1	0	
5.7	1	0	
5.8	1	0	
5.9	1	0	
5.10	1	0	

(Max Score = 10)

***If 5.5 =YES and 5.6=NO then 5.5+5.6=2**

Table 6: Access and Accuracy of Personal data

Questions For Analysis	Yes	No	N/A
6.1	1	0	
6.2	1	0	
6.3	1	0	
6.4	1	0	
6.5	1	0	
6.6	1	0	
6.7	1	0	1
6.8	1	0	
6.9	1	0	
6.10	1	0	

(Max Score = 10)

Table 7: Safeguarding Personal Data

Questions For Analysis	Yes	No	N/A	Provide Details
7.1	**1**	**0**		
7.2	**1**	**0**		
7.3	**1**	**0**		
7.4	**1**	**0**		
7.5	**1**	**0**		
7.6	**1**	**0**		
7.7	**1**	**0**		
7.8	**1**	**0**		
7.9	**1**	**0**		
7.10	**1**	**0**		

(Max Score = 10)

Table 8. Anonymisation Process

Questions For Analysis	Yes	No	N/A
8.1	1	0	
8.2	1	0	
8.3	1	0	
8.4	1	0	
8.5	1	0	
8.6	1	0	
8.7	1	0	
8.8	1	0	
8.9	1	0	

(Max Score = 9)

Table 9: Openness, Transparency & Public Engagement

Questions For Analysis	Yes	No	N/A
9.1	4	0	
9.2	1	0	
9.3	1	0	
9.4	1	0	
9.5	1	0	
9.6	4	0	

(Max Score = 12)

If 9.2=YES + one among 9.3, 9.4, 9.5=YES, then 9.2+9.3+9.4+ 9.5=4

If 9.2=NO, then 9.3, 9.4, 9.5=N/A

If 9.2=YES and 9.3, 9.4, 9.5=NO, then 9.2=2

Table 10. Transparent Health Research Projects Approval Process

Questions For Analysis	Yes	No	N/A
10.1	1	0	
10.2	1	0	
10.3	1	0	
10.4	1	0	
10.5	1	0	
10.6	1	0	
10.7	1	0	

(Max Score = 7)

Table 11. Beneficence/Non-maleficence Principles in Health Research Project Approval Processes

Questions For Analysis	Yes	No	N/A
11.1	1	0	
11.2	1	0	
11.3	1	0	
11.4	1	0	
11.5	1	0	
11.6	1	0	
11.7	1	0	
11.8	1	0	**1**
11.9	1	0	
11.10	1	0	1

(Max Score = 10)

References

1) Di Iorio CT et All. Cross-border flow of health information: is 'privacy by design' enough? Privacy performance assessment in EUBIROD. Eur J Public Health. 2013;23(2):247–53.

2) Di Iorio CT et al. Privacy Impact Assessment Report: “Privacy Performance Assessment” of EUBIROD Registers, EUBIROD Consortium, March 2012 Update. Available at: http://www.eubirod.eu/documents/downloads/D5.2_final_update_2012.pdf

3) OECD. Strengthening Health Information Infrastructure for Health Care Quality Governance: Good Practices, New Opportunities and Data Privacy Protection Challenges (2013) OECD Health Policy Studies. Available at: http://www.oecd.org/publications/strengthening-health-information-infrastructure-for-health-care-quality-governance-9789264193505-en.htm

4) OECD, Health Data Governance: Privacy, Monitoring and Research, OECD Health Policy Studies, Paris: OECD Publishing, 2015. Available from http://dx.doi.org/10.1787/9789264244566-en

5) OECD, Recommendation of the OECD Council on Health Data Governance, The Next generation of Health Reforms, OECD Health Ministerial Meeting, 17 January 2017. Available at: http://www.oecd.org/els/health-systems/health-data-governance.htm

6) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

7) Di Iorio CT et all(2009) Privacy impact assessment in the design of transnational public health information systems: the BIRO project, Journal of Medical Ethics, Dec;35(12):753-61

8) Estupiñán Romero FR,Baixauli Pérez C,Bernal Delgado E on behalf of the ECHO consortium, Handbook on methodology: ECHO information system quality report, EUROPEAN COLLABORATION FOR HEALTHCARE OPTIMIZATION (ECHO), April 2014, Available at: http://www.echo-health.eu/handbook/documents/ECHO%20INFORMATION%20SYSTEM%20REPORT%20FINAL.pdf

9) EuroHOPE (European Health Care Outcomes, Performance and Efficiency) project website, Available at: http://www.eurohope.info/index.html