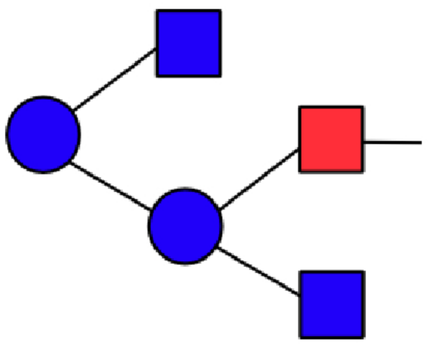

Serectrix

Supporting Decisions

www.serectrix.eu

Privacy and Ethics Impact & Performance Assessment (PEIPA)

Questionnaire

Dr. Concetta Tania Di Iorio

Legal Consultant LL.M M.P.H.

Serectrix snc

Email: ct.diiorio@serectrix.eu

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[3,4,5,6].

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.

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?				

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