CODE of PRACTICE on SECONDARY USE of MEDICAL DATA in SCIENTIFIC RESEARCH PROJECTS

TABLE OF CONTENTS

VERSION HISTORY

Version	Publication Date	Summary of Substantial Changes
IMI2/INT/2014-02972	27 Aug 2014 Final Draft	Not applicable

DISCLAIMER[1]

This document contains general information about legal matters. The information is not advice, and should not be treated as such. The legal information in this document is provided "as is" without any representations or warranties, express or implied. Authors and reviewers make no representations or warranties in relation to the legal information in this document. Without prejudice to the generality of the foregoing paragraph, authors do not warrant that the legal information in this document is complete, true, accurate, up-to-date, or non-misleading.

Legal advice shall only be provided by your legal department and in no case the information herein presented shall be viewed nor treated as an alternative.

If you have any specific questions about any legal matter you should consult your attorney or other professional legal services provider. You should never delay seeking legal advice, disregard legal advice, or commence or discontinue any legal action because of information in this Code.

Nothing in this legal disclaimer will limit any of our liabilities in any way that is not permitted under applicable law, or exclude any of our liabilities that may not be excluded under applicable law.

[1] Disclaimer adapted from a Contractology template available at http://www.freenetlaw.com

INTRODUCTION

This Code of Practice aims to provide a set of harmonised rules applicable to secondary use of medical data. It is intended to be useful to research projects involving multiple legal entities established in one or more EU member countries.

Secondary use of data occurs when data is used for a purpose different from the purpose for which the data was initially collected. Enabling secondary use of medical data by healthcare professionals and researchers is important to improve the quality of health care and research effectiveness. At the same time, it is important to protect patient privacy and to ensure that no harm is done to a patient through the use of the data.

The discipline of translational medicine[2] is growing rapidly. Therefore the secondary use of individual-level medical data and human biological samples has become increasingly necessary for progress. This has raised operational concerns in the existing regulatory context.

The EU has made progress in harmonizing the rules on the processing of personal data[3]. Nevertheless there remain differences in the way EU member states and individual organizations interpret and apply these rules.

In practice, it therefore has proven difficult for research projects such as the projects funded by the Innovative Medicines Initiative to set-up an approach to deal with the

[2] Translational medicine is a discipline within biomedical and public health research that aims to improve the health of individuals and the community by "translating" findings into diagnostic tools, medicines, procedures, policies and education. It requires linking data from clinical trials and health care with data from fundamental research programs.

[3] Directive 95/46/EC Of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

secondary use of personal medical data which is common to all partners. More importantly it is well recognized by such projects that is a recurrent challenge[4].

This Code of Practice[5] aims to provide multi-partner, multinational scientific research projects with urgently needed practical guidance compliant with the current applicable laws.

CONTRIBUTORS

The development of this Code was initiated by Anne BAHR (R&D Privacy Officer – Sanofi; Member in 4 IMI projects). It was developed with Irene SCHLUENDER (German Lawyer – TMF; Member in 2 IMI projects), Leila EL HADJAM (Data Protection Analyst – EISBM; Member in 1 IMI project) and Ann MARTIN (IMI Office coordinator for several IMI Knowledge Management projects). It was submitted for review to 2 external experts, Jean-Marc van Gyseghem (Privacy Director – Namur University) and Nikolaus Forgo (Professor of Law – Leibniz University Hannover; supported by Stefanie Hänold (Lawyer – Member of an FP7 project)).

Many other persons, who are involved in various collaborative research projects, also contributed by commenting parts of this Code. The authors of this Code would like to thank them very much for their helpful comments and apologise if having forgotten any person:

- Charles AUFFRAY – Head of EISBM @ CNRS,
- Gokce BANU LALECI ERTURKMEN – Senior Researcher at SRDC,
- Brenban BARNES – EFPIA Director of IP & Global Health,
- Jay BERGERON – Director of Translational and Bioinformatics @ Pfizer,
- Ruth CHADWICK – Professor @ Cardiff University,

[4] During a round table of 11 publicly funded European research projects on common issues (Convergence meeting November 2012) it was recognized that each project has technical or legal issues for sharing personal medical data due to different national implementations of Directive 95/46/EC. Moreover consent management is resource intensive effectively stopping meaningful re-use of medical data for new scientific research.

[5] Directive 95/46/EC Recital (26) foresees the development of Codes of Conduct.

- Gerry DAVIES – Senior Lecturer @ University of Liverpool,
- Paul DODSON – Global Service Delivery Lead R&D Information @ AstraZeneca,
- Persephone DOUPI – Senior Researcher @ National Institute for Health and Welfare,
- David HENDERSON – Principal Scientist @ Bayer,
- Dipak KALRA – Clinical Professor of Health Informatics @ UCL,
- Gunnar KLEIN – Professor of Informatics/ eHealth @ Örebro University,
- Nathalie JULLIAN – Senior Project Manager @ EISBM,
- Judith JUNK – Legal Counsel @ Bayer,
- Eugenia LAMAS – Researcher on Ethics @ INSERM,
- Pierre-Yves LASTIC – Sanofi Chief Privacy Officer,
- Paul LAWTON – UK Council for Health Informatics Professions (UKChip),
- Iheanyi NWANKWO – Leibniz University Hannover,
- Estefania RIBEIRO – IMI Data Privacy Officer,
- Fabien RICHARD – Principal Scientist @ Merck KGaA,
- Mansoor SAQI – Senior Scientist @ EISBM,
- Peter SINGLETON – Director @ Cambridge Health Informatics,
- Marc STAUCH – Leibniz University Hannover,
- Jill Nina THEURING – Legal Counsel @ Bayer,
- Emmanuel VAN DER STUYFT – Pharma IT Manager @ J&J.

DEFINITION OF TERMS

The definitions below shall be considered only for the purpose of this Code.

Definitions indicated with * are reproduced or adapted verbatim from Directive 95/46/EC Recital 26, Article 2 (a, b, d, e, f), or Article 28.

AGGREGATED DATA	Data of several individuals that have been combined to show general trends or values.
ANONYMISATION*	Process of removing all elements allowing the identification of an individual person (i.e., of rendering data anonymous).
ANONYMISED DATA	Data which was identifiable when collected but which are not identifiable anymore (have been rendered anonymous). Anonymous data are no longer personal data.
CLINICAL TRIAL	Any investigation in human subjects intended to discover or verify the effect of one or more investigational health interventions (e.g., drugs, diagnostics, devices, therapy protocols) that generate safety and efficacy data before making the health intervention available in health care[6].
DATA CONTROLLER (or Controller)*	The natural or legal person, or any other body, which alone or jointly with others determines the purposes and means of the processing of personal data[7].
DATA PROCESSOR (or Processor)*	The natural or legal person, or any other body, which processes personal data on behalf of the controller.
DATA SUBJECT	The person whose personal data are collected, held or

[6] Adapted from its definition in Directive 2001/20/EC of 4 April 2001 ("on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use"). This includes clinical trials carried out in either one or multiple sites, whether in one or several countries.

[7] In a clinical trial, the organisation(s) responsible for the trial is usually considered being the controller (for collaborative projects, see EDPS "Opinion related to the clinical study in the frame of the research project PROTECT WP4", issued on 29 November 2012)

	processed[8].
DE-IDENTIFICATION	Process of rendering data pseudonymised or anonymised.
GENETIC DATA	All personal data relating to the genetic characteristics of an individual which have been inherited or acquired as they result from an analysis of a biological sample from the individual in question, in particular by chromosomal, desoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis or analysis of any other element enabling equivalent information to be obtained[9]. This Code considers only genetic data rich enough to identify a data subject.
HUMAN BIOLOGICAL SAMPLE	Any biological material collected from human (including blood, sputum, extracted DNA/ RNA, etc.).
INCIDENTAL FINDING	Previously undiagnosed medical conditions that are discovered unintentionally and are unrelated to the current medical condition which is being treated or tests being performed[10].
MEDICAL DATA	Any data concerning patients or study participants health, collected within the context of health care or clinical trials (e.g., name, address, living conditions, health data, life style habits, social security number, image data…)[11].
PERSONAL DATA*	Any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Also

[8] See European Data Protection Supervisor, retrieved 06/08/2014
[9] As defined in Article 4 para (10) of "General Data Protection Regulation" voted by the parliament
[10] See Incidental findings, retrieved 06/08/2014
[11] Unless otherwise specified, medical data refers to individual subject data and not aggregated subject data.

	commonly referred to as Personally Identifiable Information or PII[12].
PROCESSING*	Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaption or alteration, retrieval, consultation, use disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
PROSPECTIVE DATA COLLECTION	Data needed for the specific research project which have not yet been collected or are not yet part of another research project. In contrast, retrospective data has already been collected for another research project or for health care (i.e., requiring secondary use of data).
PSEUDONYMISATION	Process of removing all elements allowing the identification of an individual person, except the key(s) allowing linking the data to the person. Such key shall be randomly generated and subject to technical and organisational measures to prevent its unauthorised use.
PSEUDONYMISED DATA	Personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution. The only difference between pseudonymised and anonymised data is that in the latter case there exists no key to link data to the data subject
RE-IDENTIFICATION	The process of linking de-identified data to the study participant.
RESEARCH	Any scientific research project including clinical trials and fundamental research, aiming at gaining scientific

[12] Many guidelines use the term Personally Identifiable Information or PII

	knowledge in the health sector.
SECONDARY USE OF DATA (or Data Re-Use)	Processing of already existing medical data for a purpose different from the purpose for which they have been initially collected[13].
STUDY PARTICIPANT	Any person participating in a research study, whether or not a clinical trial. It can refer to patients or healthy volunteers (it does not include health care professionals).
SUPERVISORY AUTHORITY*	The public authority (or authorities) in each member state responsible for monitoring the application of the administrative measures and regulations adopted within their member state pursuant to the Data Protection Directive. In this code, additionally other supervisory authorities may be considered e.g., the European Medicines Agency.
THIRD PARTY*	Any natural or legal person other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data.
TRUSTED THIRD PARTY	The person or body that, in the case of pseudonymised data, is in charge of holding the key so as to safeguard the privacy of the patient or study participant[14]. The trusted third party has to act in an independent manner. It ensures that the re-identification key is not disclosed to anyone not authorised to access.

[13] E.g., medical data collected to conduct a clinical trial on breast cancer used to run a study aiming to identify new biomarkers, but which was not planned in the consent form

[14] The Trusted Third party is responsible for keeping the "pseudonymising key" and shall not disclose it to anyone, unless otherwise authorised.

ARTICLE 1 - General Provisions

1. SCOPE

This Code aims at addressing the processing of personal medical data (pertaining to one or multiple persons) to be used or re-used in collaborative research projects.

This Code is designed to be inter alia compliant with:

- Article 8 of the European Convention on Human Rights
- Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981 (convention 108)
- Charter of Fundamental Rights of the European Union 2010/C 83/02[15]
- Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

2. ADHERENCE

Where applicable, adherence to this Code can be effective by reference to it in a legally binding document, contract or unilateral declaration (see Appendix 1).

This Code strictly aims at facilitating compliance with applicable legislation. The term "shall" in this Code means the action is obligatory.

[15] In particularArticle 8

ARTICLE 2 - Collection, Use and Transfer of Personal Medical Data

RULE 1: The Data Controller of the legal entity making personal data available to recipient(s) of another legal entity for the purposes of a scientific project shall verify that:

- The data collection complied with the applicable legal and ethical requirements, and,
- The secondary use and/or transfer of the data meet current legal and ethical requirements[16].

RULE 2: The entity which provides personal data to recipient(s) of another legal entity for the purposes of a scientific project shall inform the project of any restriction of use or obligation applicable to these data (e.g., the limited scope of purposes imposed by the consent form, the obligation to report incidental findings, etc.).

RULE 3: The secondary use of medical data in scientific research projects shall take place using anonymised data. If it is impossible to achieve the purposes of the research using anonymised data, this shall be justified and documented and pseudonymised data shall be used[17].

RULE 4: All the cases where a controller takes action in order to make personal data available to a third party located outside the European Union shall be considered a

[16] In practice this means that the controller needs to verify legal and ethical requirements subject to the recipient(s) especially if located in another member state.

[17] Any exception to this rule shall be based on applicable law. In some countries, directly identifiable data can be used in research projects when this use is specifically authorised for the planned research. Such use can be either be authorised by a specific law or by a supervisory authority (e.g., a Data Protection Supervisory Authority).

transfer[18] in the meaning of Directive 95/46/EC Article 25. Such transfer is forbidden, unless appropriate safeguards are provided (e.g., if EU model clauses have been implemented and the transfer has been authorised by the competent supervisory authority).

RULE 5: Pseudonymised data can be shared outside the European Union[19] if handled in compliance with RULE 10.

RULE 6: Transfer of personal data to third parties shall comply with RULE 1 and require that the maintenance of the protection of Personal Data is guaranteed by the recipient[20].

ARTICLE 3 – De-identification and Protection of Anonymised Data

RULE 7: In order to pseudonymise or anonymise personal data, state of the art de-identification measures have to be taken to remove and/or to conceal sufficient direct and/or indirect identifiers (see Appendix 3)[21]. The number and the selection of identifiers to be removed, depends on the risk for privacy violations. The data

[18] As defined in the EC document entitled "Frequently asked questions relating to transfers of personal data from the EU/EEA to third countries". This includes remote access to personal data to a third party located in a third country

[19] Even though it is not always implemented in law, it is generally considered by Personal Data Protection Authorities, and confirmed by Art29WP's opinion 136, that pseudonymised personal data shall not require application of the Directive 95/46/EC Article 25 if compliant with RULE 10.

[20] Planned transfer to third parties should be part of the notification to the competent supervisory authority (if notification is required) and in the information sheet for the data subject.

[21] As a result, the only difference between pseudonymised and anonymised data is the identifying key table: pseudonymised data become anonymised data if the identifying key table is destroyed.

controller shall document the de-identification methods applied and ensure that the identifying key is securely stored (or destroyed in case of anonymisation)[22].

RULE 8: Initial pseudonymisation and anonymisation of directly identifiable medical data shall only be performed by someone bound to medical or clinical secrecy (e.g., a health care professional)[23].

RULE 9: Further de-identification[24] of data shall only be done by persons authorised to have access to the data and bound to confidentiality.

RULE 10: Personal Data which have been pseudonymised shall not be considered personal data in the hands of a user who does not have access to the key if:

- The de-identification process is compliant with RULE 7, and,
- A binding agreement defines the conditions under which the data can be used[25], and,
- Appropriate technical measures have been taken to minimize risk of re-identification, as set out in Article 6.

RULE 11: Anonymisation of personal data is considered further processing which is compatible[26] with the purpose for which the data were originally processed[27].

[22] De-identification methods inevitably lead to loss of precision of the data. Pseudonymisation allows a research project to apply to a data controller to obtain higher precision data according to a specific analysis plan (e.g., modelling in a small population).

[23] Unless otherwise permitted by law.

[24] E.g., Clinical trials data are subject to the clinical trial Directive 2001/20/EC and regulation N° 536/2014 requiring retention of specific data by the sponsor. They need further de-identification in order to be regarded as pseudonymous or anonymous in the sense of this Code.

[25] Attempt to re-identify the data subject should be forbidden and may be included in a binding agreement

[26] Unless anonymisation of the data is obvious abuse or explicitly prohibited in e.g., the consent form.

[27] This means that consent is not required for anonymising personal data. Nevertheless, it is good practice to notify the data subject in the study information sheet that any data related to his/her person may be de-identified and the identifying key destroyed.

RULE 12: Aggregated data are considered anonymous data provided safeguards are taken to avoid the risk of re-identification of data subjects (e.g., in case of low cell counts, rare disease).

RULE 13: Anonymised medical data can be used for research without consent or legal basis. They should however remain protected, considering future risks of identification[28].

ARTICLE 4 - Information, Consent and Withdrawal

1. BASIC INFORMATION AND CONSENT FOR PROSPECTIVE DATA COLLECTION[29]

RULE 14: Data controllers prospectively collecting personal data shall inform the study participants comprehensively and appropriately about the[30]:

- Identity of the data controller, and,
- Purposes of the processing, and,
- Potential implications for the study participant, and,
- Recipients of the data, and,
- Possibility to be contacted after the study, and,
- Existence of the right of access to, and the right to rectify the data.

The study participants' information shall also cover:

[28] What today seems to be anonymised data may change depending on what other data may become available on the data subject(s) and the development of information and communication technologies. As the disclosure of medical data may harm the data subject(s) significantly, it is good practice to protect even "anonymous" medical data.

[29] See Appendix 2 for concrete examples

[30] In case of inclusion of data subjects in a national register, study participants must also be informed about this register.

- What data will be processed, and,
- Whether and how project results/ incidental findings will be communicated, and,
- Whether data will be pseudonymised or anonymised, and,
- Whether that participation is voluntary or not, and,
- Where applicable that:
    - The patient has the right to withdraw from the study at any time, and,
    - That genetic analyses may be conducted, and,
    - There is a transfer of data to a processor or to a third-party or to a country located outside of the European Union.

The information shall also include the fact that data might be anonymised and that consent withdrawal is only effective according to rules laid down in RULES 23 and 24, as long as data remain identifiable.

RULE 15: The data controller shall ensure that study participants provide their informed consent, preferably in writing, on the basis of the information defined in RULE 14.

RULE 16: In order to enable new research on the basis of secondary use of medical data, consent forms used in projects collecting data should cover secondary use[31].

2. PROJECT RESULTS

RULE 17: Results or outcomes from a research project should be made available to study participants in a manner allowing non-specialists to understand the study results[32].

[31] Examples of information sheet and consent form are provided as Appendix 2

[32] This does not apply to results for an individual study participant but to the overall results of the research project; it does not mean that results are proactively sent to study participant but that they are made accessible in a place the study participants have been informed about

3. INCIDENTAL FINDINGS

RULE 18: The research project shall, where applicable, define rules to deal with incidental findings (e.g., to communicate the finding to the initial controller[33]).

4. SECONDARY USE OF HEALTH CARE DATA IN RESEARCH PROJECTS[34]

RULE 19: Personal medical data collected for health care purposes (e.g., data registered in hospitals' electronic health record systems) shall only be re-used for research projects if[35]:

- The secondary use is covered by the patient's consent, or,
- Secondary use of health care data without consent is permitted by an applicable law[36] or by a competent data protection supervisory authority.

5. SECONDARY USE OF RESEARCH DATA

RULE 20: Personal medical data already lawfully collected for research purposes, including data arising from clinical trials, can be re-used in another research project if:

- The initial consent covers the possibility of re-use, or,
- The data have been de-identified according to RULE 10 and the initial consent does not explicitly forbid the planned secondary use, or,
- Permitted by an applicable law.

[33] The initial controller is the one who has the duty to handle incidental findings according to the initial consent and protocol, as well as the applicable laws. In order to be in a fair situation to deal with such question, the case must have been planned in the protocol and the informed consent form, e.g., by informing the study participant of the means for being or not being informed in such cases

[34] See Appendices 4 and 5 for more details on conditions for secondary use of personal medical data

[35] In such cases, it is good practice to inform patients of the secondary use of their data (e.g., on a website, by a patient information tool, by a notice in the waiting room or a note in the hospital welcome leaflet provided to each patient), and of their right of access, correction and opposition as well as of the means for opting-out

[36] Most often, the applicable personal data protection law is the law of the country in which the data controller is established. For more details, see "Opinion 8/2010 on applicable law adopted on 16 December 2010 by the Article 29 Working party"

6. SECONDARY USE OF GENETIC DATA

RULE 21: Genetic data which is rich enough to single-out a person (e.g., a whole genome sequence) shall always at a minimum be subject to the safeguards applicable to personal data[37].

RULE 22: Genetic data which is rich enough to single-out a person shall be re-used for purposes not covered by the initial consent only if[38]:

- The new purpose is of substantial public interest[39], and,
- Data have been de-identified according to RULE 7, and,
- Data use is compliant with RULES 10 and Article 6, and,
- Users are subject to a policy prohibiting any attempt to re-identify data subjects, and,
- This specific secondary use is not forbidden by applicable law, neither by the initial consent.

7. CONSENT WITHDRAWAL

RULE 23: Study participants have the right to withdraw their consent at any time without justification.

RULE 24: In case study participants withdraw their consent for use of their data[40], data and derived results shall be erased from all research project databases[41] except

[37] As DNA is a key that allows to uniquely and permanently identify a person, this rule shall apply even if related data have been anonymised

[38] The current legal framework in Europe does not clearly allow the secondary use of genetic data which is rich enough to single-out a person without consent for the re-use. This is a crucial issue for conducting research in Europe. It becomes critical that new provisions are developed at the European level to allow such re-use under very clear conditions balancing privacy and research interests. RULE 22 would according to this code allow the secondary use of Genetic data rich enough to re-identify a person under strict secure conditions, whereas without this Code, it would not be possible unless new consent is given.

[39] Scientific Research Projects funded through public research programs are motivated by public interests and hence can be considered of substantial public interest e.g., the projects funded through the IMI

[40] It has to be noted that from a statistical point of view it is important to maintain the data from subjects withdrawing from a study to understand any potential bias in the overall study results due to withdrawal. A

where applicable law requires the maintenance of the data (e.g., adverse event reporting).

ARTICLE 5 – Human Biological Samples

1. COLLECTION OF HUMAN BIOLOGICAL SAMPLES AND CONDUCT OF GENETIC ANALYSES

RULE 25: The collection of human biological samples can only be undertaken if the consent of the donor covers this collection, or if otherwise permitted by applicable laws. The donor shall be informed as stated in RULE14.

RULE 26: The genetic analyses of human biological samples can only be undertaken if such analyses are not prohibited by applicable laws and:

- The consent of the donor covers these genetic analyses, or,
- When the donor cannot with reasonable means provide consent, the national law/ the competent supervisory authority allows for the re-use and related data have been de-identified according to RULE 7[42].

minimum is to maintain the data up to the point of withdrawal from the study and documentation of the reason(s) for withdrawal.

[41] Withdrawal for using data or samples will only be possible if the study participant is still identifiable in the database. The health care professional receiving the request should clarify the wish of the study participant, e.g., stopping taking part in an on-going study, asking to delete his/her data, etc.. If there is no specific documentation, it should be considered that the study participant wanted to stop taking part from that point onwards in the study. If withdrawal of data, the data controller is responsible for ensuring that all data listed to be withdrawn are deleted, unless an applicable law would prevent it (in such case the study participants should be informed).

42 E.g., such a law exists in Germany. In many EU countries in order to make genetic analyses possible the consent must explicitly specify that such analyses may take place (e.g., France, Italy). This includes cases where the consent allows to use the material for broad purposes (e.g., for biobanking). Therefore it is strongly recommended to include information on potential genetic analyses in the consent form of any project in which human biological samples are collected (even though genetic analyses are not planned yet) as genetic material can be extracted from nearly all human biological samples and some genetic analyses may become necessary for the new research project

2. SECONDARY USE OF HUMAN BIOLOGICAL SAMPLES

RULE 27: If the initial consent did not cover the secondary use of samples, samples can only be re-used if:

- Donors' initial consent did not prevent the secondary use, and,
- The secondary use is permitted by law or by the competent supervisory authority[43].

RULE 28: In case donors withdraw their consent for use of their samples, all samples and derivatives shall be destroyed in the research project[44].

ARTICLE 6 - Data Security & Involvement of Data Processors

RULE 29: Appropriate technical and organizational measures shall be implemented to protect personal data against accidental destruction or loss, alteration and unauthorized disclosure or access[45]. This requires in particular:

- The enforcement of a policy for the confidentiality, protection and security of data, including documented training on the policy.
- Computerised systems which are access controlled and protected against physical and electronic intrusion, and,
- Technical security measures complying with the relevant guidance and regulations applicable, for instance, to clinical trials.

[43] Depending on the countries, it could be an ethics board or a state agency

[44] If the samples of the donor can still be identified and unless applicable law requires maintenance of the data. The entity which collected the sample is responsible for ensuring compliance with this rule unless otherwise defined.

[45] As defined in Article 17 (1) of Directive 95/46/EC. Privacy regulations require these principles to apply only to personal data, thus not on anonymous ones. However to ensure the integrity of research results it is strongly recommended to apply these principles to all research data.The implementation of the access policy and technical security measures should be documented.

RULE 30: The carrying out of processing by way of a processor[46] shall be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

- The processor shall act only upon instructions from the controller, and,
- The obligations set out in RULE 29 shall also be incumbent on the processor[47].

RULE 31: The controller shall ensure[48] that the processor provides sufficient guarantees regarding technical and organizational security measures, in accordance with the RULE 29.

ARTICLE 7 - Documentation and Data Retention

RULE 32: Any secondary use or sharing of data with third parties shall be documented[49].

RULE 33: Research data related to scientific publications should be retained long enough to ensure reproducibility and verifiability of the findings[50], wherever possible in anonymised format but otherwise subject to pseudonymisation. This equally applies to any study results described in a report.

[46] If a member of a consortium is in charge of a specific task (e.g., providing data hosting services), this member shall be considered a processor for the other members and comply with this article.
[47] As defined in Article 17 (3) of Directive 95/46/EC
[48] It is recommended for the controller to audit new service provider (e.g., verify the quality plan of the company, the validation of the computer systems, the existence of a back-up and a data recovery system).
[49] In practice, each adherent shall document which data (e.g., a given clinical study database) have been shared (regardless whether it is anonymous or not). This information shall include at least the purpose, the recipients and the date of sharing
[50] Institutions must ensure that data are retained not just to the end of the project but as long as scientifically relevant and in a machine-readable format

RULE 34: Retention periods should be defined before processing personal medical data according to its purpose and applicable law[51]; retention period shall be communicated to any third party to whom the data shall be transmitted.

RULE 35: Pseudonymised research data may be stored on the computer systems of the member organisations or of their authorised partners/ processors/ third-parties, as long as it may be required for further lawful research, subject to on-going appropriate technical and organisational safeguards.

RULE 36: Anonymous research data may be stored as long as necessary.

ARTICLE 8 – Medical Data Disclosure

RULE 37: Pseudonymised data shall not be publicly disclosed.

RULE 38: Anonymised data disclosure shall follow state of the art de-identification methods (see Appendix 3) according to the following principles:

- Disclosure of such data shall be justified by a clear scientific rationale.
- De-identification is performed in a way that reduces the risk of the data being associated with an individual subject to a minimum, and,
- Publication on public servers is subject to a documented risk assessment[52] including appropriate approvals, and,
- Where data is disclosed to third parties, these parties are subject to an agreement (which might be available on-line and for free) and which forbids

[51] As defined in Article 6 (e) of Directive 95/46/EC, personal data shall not be kept in a form which permits identification of patients or study participants for longer than is necessary for the purposes for which the data were collected. Data can be anonymised to increase the retention period.

[52] The risk assessment weighs up the scientific benefits of making the data public against the increased privacy risks and sets out how these risks can be reduced to an acceptable minimum. The risk assessment will be documented by the data controller(s).

them from attempting to re-identify subjects and to share these data with other third parties, and,

- Appropriate state of the art data security measures are taken, including control and monitoring of data downloads, and,
- The project (or after its termination, the entity in charge of providing access to the data) ensures that the risk of potential re-identification of the data remains limited with reasonable means[53].

RULE 39: Accountability for maintaining disclosed data anonymous (i.e., not re-identifiable) shall be clearly assumed by the relevant data controller(s). In the event that the risk of re-identification becomes unacceptable, the controller(s) should deny and/or revoke access to such data.

ARTICLE 9 - Implementation of the Code Rules

RULE 40: All partners of a collaborative scientific research project shall sign a binding agreement setting out different roles and responsibilities with regards to the processing of personal data[54], or include this provision in another binding document[55].

RULE 41: Each entity processing personal medical data should:

[53] If data are being disclosed on public servers, the review frequency as well as the entity in charge should be defined in a binding agreement. If re-identification would become possible with reasonable effort, further anonymisation procedures should be applied. If not possible or requiring disproportionate efforts, data should be removed from the public servers.
[54] E.g., a Memorandum of Understanding, as recommended by the EDPS for the IMI PROTECT project
[55] Within the project, all professionals (e.g., physicians) are additionally committed to the ethics and code of conduct existing in their field of practice

- Establish internal procedures to transpose personal data protection rules into binding requirements or to make this Code (see Appendix 1) binding, and,
- Where necessary, anticipate and define specific rules (e.g., sanctions), and,
- Ensure that the procedures are implemented and easily accessible to all persons having access to personal medical data.

ARTICLE 10 - Code modifications

This Code of Practice will be reviewed and revised periodically by a panel of scientific, data protection and ethics experts to ensure continued compliance with EU directives and regulations. This periodic review will be organized by the IMI Programme Office.

Each version of the Code will be clearly labelled and referred to with a Code version number, the date of publication and a summary of the substantial changes.

APPENDICES

Appendix 1: Adherence Agreement (given as an example for projects which are willing to render this Code binding)[56]

Mr. / Ms. [First Name, Last Name],

acting on behalf of [Firm / legal entity], holding the position of [position] herewith declares:

- I have the legal capacity to represent and engage [Firm/legal entity] for the purpose of this project.
- [Firm] agrees to fully endorse and adhere to the [Code full name], Version [Version] of [date]. It shall apply to all data processing activities carried out within the project [Project name]. The personal data protection framework is thus in part formalized through this Code.
- [Firm] will ensure the implementation of all measures required by the provisions of this Code.
- [Firm] will ensure compliance with this Code by all staff and personnel working within the project on behalf of [Firm].

In addition to the rules laid out by the [Code], the following project specific rules shall apply:

- [To be developed as needed for each project]

Signed on behalf of [Firm name] on [Date] by [print name]: _____
Signature

[56] For new project, the easiest would be to include this in the project agreement

Appendix 2: Example of information sheet and consent form

These templates are given as examples. If you want to use them, you will have to adapt the content to your specific study as well as to ensure the reuse does not infringe copyright.

For conducting a clinical study

TMF[57] adapted Informed Consent Form (German version available here: http://pew.tmf-ev.de/)

TMF - ICF

WHO Informed Consent Form:
http://www.who.int/entity/rpc/research_ethics/InformedConsent-clinicalstudies.doc?ua=1

For conducting a research project (not a clinical trial)

WHO Consent for Storage and Future Use of Samples:
http://www.who.int/entity/rpc/research_ethics/Informed%20consent%20for%20sample%20storage.doc?ua=1

STRATUM consortium Consent for Storage and Future Use of Unused Sample (for Biobank Donors):
http://stratumbiobanking.org/docs/Biobank%20Donor%20Information%20Sheet%20and%20Consent%20Form%20STRATUM%20Template_June2013.docx

UCC (University College Cork) Consent for Use of Sample (Generic template):
http://www.google.fr/url?url=http://www.ucc.ie/research/rio/documents/InformedConsentFormTemplate.doc&rct=j&frm=1&q=&esrc=s&sa=U&ei=1hvZU9nMEKi30QWw9YGwDg&ved=0CBQQFjAA&sig2=JmOsTeq2TdMDXMMP75m0lQ&usg=AFQjCNH_v-12RPSl_rokNVh62_j_n7xs9w

[57] TMF is the umbrella organization for networked medical research in Germany. It is the platform for interdisciplinary exchange as well as cross-project and cross-location cooperation in order to identify and solve the organizational, legal/ethical and technological problems of modern medical research. Solutions range from expert opinions, generic concepts, and IT applications to checklists, practical guides, training, and consultation services. The TMF makes these solutions available to the public free of charge.

Appendix 3: Examples of de-identification methods and guidance

The risk for re-identification is dynamic and may change as technology improves and costs decrease. The following criteria may help to define which de-identification[58] and security measures shall be taken:

- How many people have access to the data?
- Are these people bound to confidentiality?
- How high is the interest in re-identification?
- What is the level of the organizational and technical protection measures?
- How long will the data be stored?
- Will the data set be enriched over time?

This also requires balancing the four following parameters:

- level of de-identification
- motives and capacity to re-identify
- risk of invasion of privacy (potential impact on person's privacy)
- level of controls/ security measures in place.

Many de-identification methods exists, including ISO standard (1), regulatory agency anonymisation guideline (2 and 3), and others published in scientific reviews (4 to 7) or on professional organisations website (8). See examples references below.

Guidances

1. ISO/TS 25237 standard on "Health informatics -- Pseudonymization"
2. ICO (UK Data Protection Agency) Code of Practice entitled "Anonymisation: managing data protection risk": http://ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation
3. Art29WP opinion 216 on "Anonymisation Technics", issued on 10 April 2014

[58] The de-identification methods proposed in this Code are consistent with the ones proposed in the United States HIPAA standard

List of useful literature

4. Iain Hrynaszkiewicz et al., "Preparing raw clinical data for publication: guidance for journal editors, authors, and peer reviewers, Brit. Med. J, 6 February 2010, Vol. 340, p. 304-307

5. Guido van 't Noordende, "Comments on the definition of personal information and on the (re)use of personal information in anonymous or pseudonymised form in the proposed general data protection regulation": http://staff.science.uva.nl/~noordend/publications/DPR-GvN-final.pdf

6. Khaled El Emam, "Perspectives on Health Data De-Identification": http://www.privacyanalytics.ca/wp-content/uploads/2013/07/Perspectives.pdf

7. Sara Hughes, Karen Wells, Paul McSorley and Andrew Freeman, "Preparing individual patient data from clinical trials for sharing: the GlaxoSmithKline approach", Pharmaceutical Statistics, Volume 13, Issue 3, pages 179–183, May/June 2014 (see anonymisation details at this address: https://www.clinicalstudydatarequest.com/Documents/Anonymisation%20of%20Clinical%20Trial%20Datasets.pdf

8. Omer Tene, "Privacy: The new generation", International Data Privacy Law, 2011, Vol. 1, No. 1, p. 15-27

9. Y. Erlich/ A. Narayanan, "Routes for breaching and protecting genetic privacy", Nature Vol. 15 (June 2014), p. 409-421

10. EFPIA Principles for responsible Clinical Trial Data Sharing: http://transparency.efpia.eu/uploads/Modules/Documents/data-sharing-prin-final.pdf

Appendix 4: Secondary use summary

Determining whether personal medical data can be re-used.

Personal medical data already lawfully collected can be re-used in a new research project if consent allows for it or if the secondary use is allowed by law or authorized by a Supervisory Authority (SA). There are however subtle differences as each type of data may be governed by specific consent requirements or specific law.

Written consent regarding the re-use of personal medical data

Consider the following classification regardless the origin of the data (healthcare, research, or genetics):

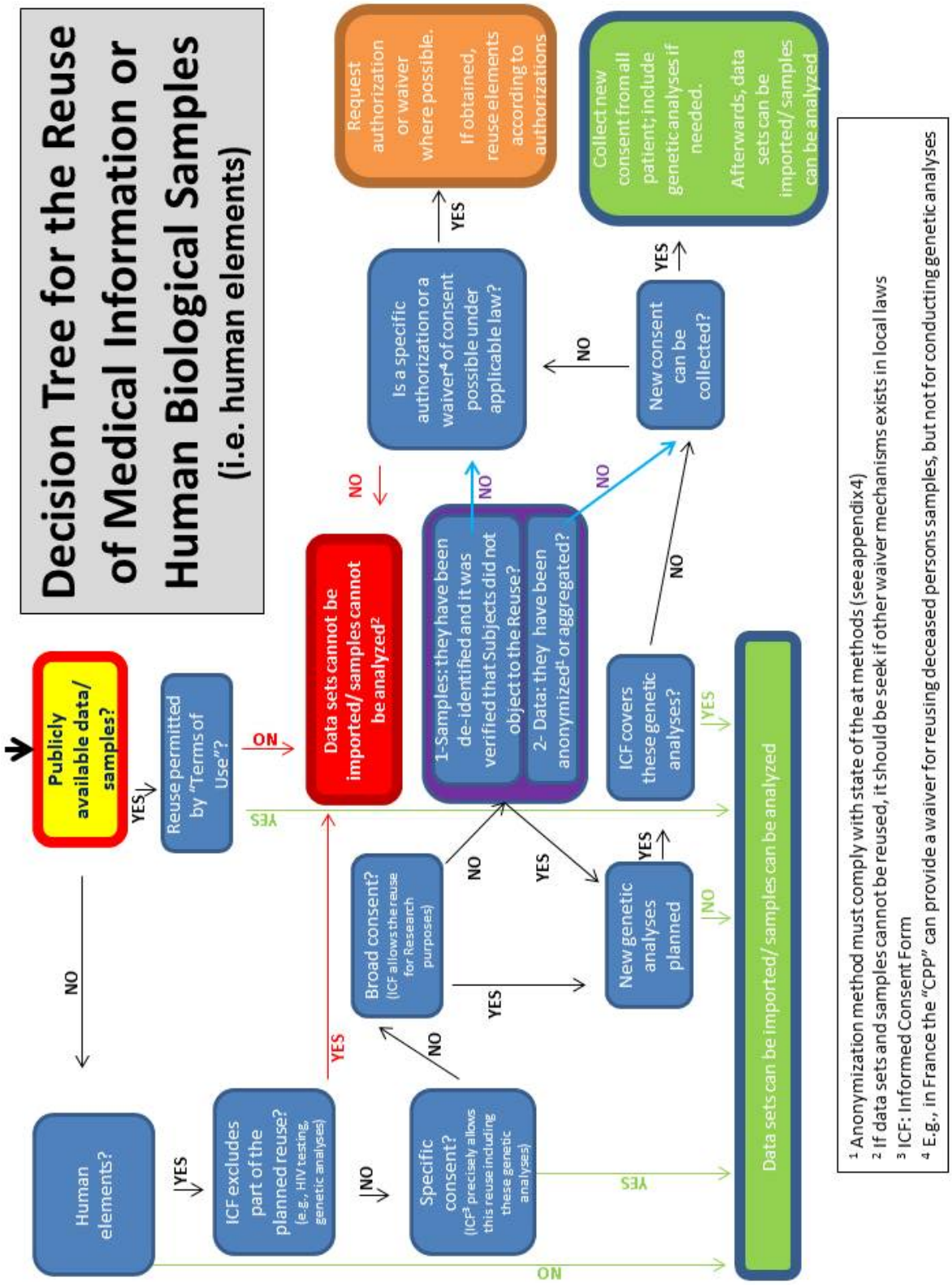
- Allows explicitly the secondary use
- Prohibits explicitly the secondary use
- Is silent (no explicit mention of secondary use) => Assume by default consent allows the secondary use.
- Is absent (no written consent) => Assume by default that there is no consent.

Allowed by:	Consent	Law or Supervisory Authority	Compliant with RULE 10 & Not prohibited by Consent
Healthcare data (RULE 19)	X	X	NO
Research data (RULE 20)	X	X	X
Genetic data (RULE 22)	X	X	X[59]

Appendix 4 also helps to make decision on secondary use through a decision tree.

[59] RULE 22 would according to this code allow the secondary use of Genetic data rich enough to re-identify a person under strict secure conditions, whereas without this Code, it would not be possible unless new consent is given.

Appendix 5: Decision Tree for Secondary Use



Additional Appendices

Additional appendices will be added to this Code in its final version, including:

- A list of use cases to provide clear examples, especially on secondary use of genetic material,
- An FAQ, to provide explanation on position taken on the most discussed RULES
- A 3-pages summary containing the rules only, to allow easy review of them