CEN

WORKSHOP

AGREEMENT

CWA 17933

June 2023

ICS 35.240.80

English version

Digital health innovations - Good practice guide for obtaining consent for the use of personal health information for research and innovations

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN-CENELEC Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No.:CWA 17933:2023 E

Contents

Page

European foreword

This CEN Workshop Agreement (CWA 17933:2023) has been developed in accordance with the CEN-CENELEC Guide 29 "CEN/CENELEC Workshop Agreements – A rapid prototyping to standardization" and with the relevant provisions of CEN/CENELEC Internal Regulations – Part 2. It was approved by the Workshop participants on 2023-05-23, the constitution of which was supported by CEN following the public call for participation made on 2022-06-13. However, this CEN Workshop Agreement does not necessarily include all relevant stakeholders.

The final text of this CEN Workshop Agreement was provided to CEN for publication on 2023-05-23.

Results incorporated in this CWA received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 857188.

The following projects, organizations and individuals developed and approved this CEN Workshop Agreement:

— ADLIFE (Grant agreement No: 875209), The European Institute for Innovation through Health Data, Dipak Kalra

— ADLIFE (Grant agreement No: 875209), Kronikgune Institute for Health Services Research, Ana Ortega

— ADLIFE (Grant agreement No: 875209), Kronikgune Institute for Health Services Research, Lola Verdoy Berastegi

— InteropEHRate (Grant agreement No: 826106), University of Vienna, Department of Innovation and Digitalisation in Law, Tima Out Anwana, Marie-Catherine Wagner, Katerina Polychronopoulos, Lukas Faymann

— KATY (Grant agreement No: 101017453), University of Vienna, Department of Innovation and Digitalisation in Law, Katarzyna Barud

— OPEN DEI (Grant agreement No: 857065), ETHEL, Luc Nicolas

— PHArA-ON (Grant agreement No: 857188), Stelar Security Technology Law Research, Matthias Pocs

— PHArA-ON (Grant agreement No: 857188), UNINFO, Fabio Guasconi

— PHArA-ON (Grant agreement No: 857188), UNINFO, Roberto Scano

— PHArA-ON (Grant agreement No: 857188), Universidade da Beira Interior, Nuno Manuel Garcia dos Santos

— PHArA-ON (Grant agreement No: 857188), University of Florence – Department of Industrial Engineering, Erika Rovini

— PHArA-ON (Grant agreement No: 857188), University of Florence – Department of Industrial Engineering, Filippo Cavallo

— PHArA-ON (Grant agreement No: 857188), UP Umana Persone Social Enterprise R&D, Gianna Vignani

— SHAPES (Grant agreement No: 857159), Medicines Optimisation Innovation Centre, Northern Ireland, Michael Scott

— SMART BEAR (Grant agreement No: 857172), National and Kapodistrian University of Athens, Eleftheria Iliadou

— SMART BEAR (Grant agreement No: 857172), University of the Basque Country, Idoia Landa

— SMART BEAR (Grant agreement No: 857172), University of the Basque Country, Itziar Alkorta

— Chino.io, Giacomo Morbitelli

— Chino.io, Jovan Stevovic

— DNV AS, Guro Meldre Pedersen

— GS1 Global Office, Christian Hay

— GS1 Global Office, Neil Piper

— HL7 Europe, Catherine Chronaki

— Kinetikos Health, Ricardo Matias

— Maynooth University - National University of Ireland, Innovative Value Institute, Mansoor Ahmed

— Mexedia Health, Pier Angelo Sottile

— Technical University of Denmark, DTU Management Institute, Henning Boje Andersen

— Technical University of Denmark, DTU Management Institute, Kathrin Kirchner

— The European Institute for Innovation through Health Data, Maria Christofidou

— UNIdoc Srl, Alessandra Picchiotti

— University of Birmingham, Theodoros N. Arvanitis

The listed projects have received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement numbers indicated.

Introduction

There are many kinds of digital health innovation being developed, evaluated, deployed, and used. These include mobile applications that allow patients to enter their health status and monitoring information. Sometimes the data will be collected automatically through wearable sensors or home installed detectors. These solutions might be in continuous or asynchronous connection to healthcare provider systems to enable health and care professionals monitoring of the incoming data streams in real time or periodically. Nowadays significant advances are being made in artificial intelligence (AI) and Internet of Things (IoT) that create a more sophisticated data fusion, analysis and advisory ecosystem. Through these, a care pathway or treatment guidance can be provided to patients and healthy individuals at a granular level, in real time, with professional oversight occurring through escalation (alerting them of readings of concern) or periodically at scheduled review sessions. These are collectively described as digital health innovations. This is a rapidly expanding field for research and product development, and inevitably these developments need to be tested before they can be marketed, approved and widely adopted.

Regardless of the consent, which is needed from the individual patient or healthy person for using well-proven (e.g. on the market) devices for collecting, processing or storing the data, a further layer of consent is needed for innovation solutions since digital health innovations are still under development or in the process of being evaluated. Each patient that uses a digital health innovation is therefore in parallel participating in a study, which goes beyond the purpose of a specific medical intervention. Explicit consent from users of the digital health innovation is often needed for these developmental stages, because the solution is not yet ready to be used as part of the routine healthcare delivery. This is unlike long established CE marked products (such as home glucose monitors, ambulatory blood pressure devices, heart rate monitors) that are issued to patients or purchased by patients directly. The usage of innovations might entail risks or disruptions to the normal pattern of care and might involve the collection of evaluation data such as usability surveys or routine use data. The intended future benefits of using the solution might also not be available to the patient because the advice generated by the solution might not yet be reliable enough to be trusted for care decision-making. It is common in pilot situations to ask the patient and/or their care giver to assess the advice generated for its integrity, plausibility and safety. There is therefore uncertainty about the advisory system under evaluation regarding its trustworthiness as well as intended benefit(s).

It is the experience of many initiatives in the digital innovation field that it is difficult to know what kinds of consent are appropriate in these situations, what permissions should be sought from pilot testing individuals, and how that consent should be framed and transparently explained. It can be challenging to appropriately frame the required consent in order to meet the immediate piloting needs as well as possible future downstream reuses of data for compatible purposes (as defined in the European Data Protection Regulation (GDPR) Art. 5.1.b regarding the compatibility of purpose). It is one challenge to secure ethics committee approval to pilot the use of a digital health innovation, but another more complex challenge is to obtain ethics committee and data protection approval to reuse the pilot data for evaluations, for future innovation enhancements and for further research (which implies the need for consent that permits a broad range of future data use purposes). The different aspects of consent that might need to be covered include:

— **care intervention,** in case the research involves possible changes to care or treatment, or change clinician behaviour, which would require human ethics approval;

— **using a novel digital health tool**, which does not change patient care but changes the methods for collecting data, delivering data or interacting between actors;

— **collecting data to study the research innovation**, including any evaluation data, and sharing amongst consortium partners, potentially cross border, outside EU etc.;

— **the downstream reuse of collected data**, potentially research that might not be anticipated at the time the consent was expected, and possibly involving sharing the data with parties and to countries that were not anticipated.

This CEN Workshop Agreement 17933 has been developed as a good practice guide to help organisations and scientific associations performing research to develop and evaluate digital health innovations to obtain the most appropriate consent that they need from individuals when piloting and evaluating digital health innovations or conducting research.

A recognised challenge is to seek consent for the data gathered through the piloting phase and through evaluation instruments to be reused as a dataset for future research by other organisations, possibly in other countries. If data reuse is intended, which it often should be, then it is appropriate to check if data reuse is covered by the initial consent or if a separate, optional, consent for that data reuse should be requested.

This guide has been produced because many contemporary initiatives have indicated there is a need for understanding as to how to seek consent in an efficient and comparable manner, how to take into account ethical and data protection requirements, word consent forms needed for the study, and obtain ethics committee approval before they begin to conduct a study.

The intention of this guide is to complement a number of European and international standards that deal with more formal considerations regarding consent for the processing of personal data.

Health services and public health research also make use of routinely collected (real-world) data for quality improvement, safety monitoring, public health surveillance and population health strategy. Public and private research organisations make use of real-world data to improve disease understanding, and to develop and evaluate new treatments and other care interventions. If they include the use of personal health data, whether fully identified or pseudonymised, the GDPR requires that these are utilised by an identified data controller or data processor thereof via a legitimate (legal) basis. This legitimate basis is frequently, but not always, informed consent from each data subject. This guide can also serve as a basis for the collection of consent for these research purposes.

1 Scope

Since digital health innovations are still under development or within the evaluation process formal consent is usually needed for all stages of the development cycle. This CEN Workshop Agreement (CWA) defines a guideline for devising, obtaining and documenting the most suitable consent for the use of digital health innovations. The guideline describes which aspects should be considered when asking for consent. It specifies the appropriate consent for different situations and how it should be framed and transparently explained. This includes seeking consent for the future reuse of collected data for additional areas of research. The document establishes how to consider ethical and data protection requirements, the wording of consent forms and obtaining ethics committee approval where applicable. Further, this document focuses on how to handle the subjects access request or withdrawal during (formative and summative) technology evaluation trials. The aim is to support researchers to ensure that the appropriate ICF (informed consent form) elements are considered. This is necessary since the presently adopted consent procedures usually concern only the specific use of data for identified and therefore foreseen purposes and are often challenged to obtain data reuse consent in a suitable way.

This document does not cover the information security safeguards that should be adopted during the data processing.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
availability
property of being accessible and usable on demand by an authorized entity

[SOURCE: ISO/IEC 27000:2018, 3.7]

3.2
anonymisation
process by which personal data is irreversibly altered in such a way that a data subject can no longer be identified directly or indirectly, either by the data controller alone or in collaboration with any other party

Note 1 to entry: The concept is absolute, and in practice, it may be difficult to obtain.

[SOURCE: ISO 25237:2017, 3.2]

3.3
clinical investigation
any systematic investigation involving one or more human subjects, undertaken to assess the safety or performance of a device

[SOURCE: EU Medical Device Regulation]

3.4
coercion
use of force to persuade someone to do something that they are unwilling to do

[SOURCE: Cambridge Dictionary, Cambridge University Press]

3.5
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: ISO 7498-2:1989, 3.3.16]

3.6
consent
freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them

[SOURCE: GDPR, Art 4(11)]

3.7
(data) controller
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

[SOURCE: GDPR, Art 4(7)]

3.8
data altruism
voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law, where applicable, such as healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest

[SOURCE: EU Data Governance Act, Art 2(16)]

3.9
data subject
identified or identifiable natural person, who is the subject of personal data

[SOURCE: ISO/TS 14265:2011, 2.10; GDPR Art 4(1)]

3.10
de-identification
general term for any process of reducing the association between a set of identifying data and the data subject

[SOURCE: ISO 25237:2017, 3.20]

3.11
dynamic consent
approach to consent that enables people, through an interactive digital interface, to make granular decisions about their ongoing participation

[SOURCE: PRICTOR, M., LEWIS, M. A., NEWSON, A. J., HAAS, M., BABA, S., KIM. H., KOKADO, M., MINARI, J., MOLNÁR-GÁBOR, F., YAMAMOTO, B., KAYE, J., TEARE, H. J. A. Dynamic Consent: An Evaluation and Reporting Framework. *J. Empir. Res. Hum. Res. Ethics*. 2020, **15**(3), 175-186. Available at: https://doi.org/10.1177/1556264619887073]

3.12
explicit consent
agreement, approval or permission that is freely and directly given, expressed either viva voce or in writing or other legally authorized signature, e.g. electronic

[SOURCE: ISO 18308:2011, 3.25]

3.13
granular consent
consent that is obtained for each purpose of the target data processing activity

3.14
informed consent
permission to perform healthcare activities, voluntarily given by a subject of care having consent competence, or by a subject of care proxy, after having been informed about the purpose and the possible results of the healthcare activities

[SOURCE: ISO 13940:2015, 11.2.6]

3.15
personal data
information relating to an identified or identifiable natural person; 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

[SOURCE: GDPR, Art 4(1)]

3.16
integrity
property of accuracy and completeness

[SOURCE: ISO/IEC 27000:2018, 3.36]

3.17
primary use
use of health data for the diagnosis, treatment and care of the individual from whom the data has been collected

3.18
privacy
right of individuals to control or influence what information related to them may be collected and stored and by whom that information may be disclosed

[SOURCE: ISO/IEC TR 26927:2011, 3.34]

3.19
processing
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

[SOURCE: GDPR, Art 4(2)]

3.20
(data) processor
natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

[SOURCE: GDPR, Art 4(8)]

3.21
pseudonymisation
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

[SOURCE: GDPR, Art 4(5)]

3.22
secondary use
processing of health data for purposes other than the initial purposes for which the data were collected

3.23
special category of data
personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

[SOURCE: GDPR, Art 9(1)]

3.24
subject
an individual who participates in a clinical investigation

[SOURCE: MDR, Art 2(50)]

3.25
transparency
information addressed to the data subject that is concise, easily accessible and easy to understand, in clear and plain language and, additionally, where appropriate, visualisation is used

Note 1 to entry: The term transparency is used in this document when referring to the concept in general without specific conformance to scope of transparency defined in the GDPR. The term "GDPR transparency" is used in this document when conformance to Articles 12 and 13 of the GDPR is intended.

[SOURCE: GDPR, Recital 58, modified – Note 1 to entry added]

3.26
vulnerable
able to be easily physically or mentally hurt, influenced, or attacked

[SOURCE: Cambridge Dictionary, Cambridge University Press]

4 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply:

AI	Artificial intelligence
CIOMS	Council for International Organizations of Medical Sciences
CTR	Clinical Trials Regulation
CWA	CEN Workshop Agreement
DGA	Data Governance Act
DPA	Data Protection Authority
EDPB	European Data Protection Board
EDPS	European Data Protection Board and the European Data Protection Supervisor
EHDS	European Health Data Space
EHR	Electronic Health Record
ENISA	The European Union Agency for Cybersecurity
FAIR	Findable, Accessible, Interoperable, Reusable
GCP	Good Clinical Practice
GDPR	European General Data Protection Regulation
HIPAA	The Health Insurance Portability and Accountability Act of 1996
ICF	Informed Consent Form
ICO	UK Information Commissioner's Office
ICT	Information and Communication Technology
IoT	Internet of things
MDR	Medical Device Regulation
PET	Privacy Enhancing Technique
PHG	Public Health Genomics
R&I	Research and Innovation
T&Cs	Terms and conditions
WMA	World Medical Association

5 Consent and legal bases

5.1 Ethical, legal and regulatory bases for consent

5.1.1 General

This guide takes into account legal acts and ethical standards in force and currently binding the entities seeking consent of individuals to ensure their participation in health research and/or to ensure that their personal data can be processed in the course of research activities. It is useful to distinguish ethical and privacy safeguards. Ethical safeguards primarily seek to ensure an individual is not directly harmed through participation in research. Data protection and privacy safeguards seek to ensure an individual's privacy is respected and that they do not have the risk of harm through the inappropriate disclosure of personal information. Both aspects need to be covered when obtaining consent.

Table 1 below lists some of the most important instruments that are applicable in Europe (some are world-wide) to these two areas of safeguard from harm. In this table, the international guidelines are shown, for the sake of simplicity, as separate from the legislative framework of personal data protection. At the same time, this illustrates the fact that the standard concept of informed consent, originally tied to consent to participating in a trial with adequately described and transparently communicated risks, has grown to include consent to recording and use of personal data.

Table 1 — Ethical, legal and regulatory bases for consent

<table>
<tr><th></th><th>Protection against harm</th><th>Protection against breach of privacy</th></tr>
<tr><td rowspan="3">Ethical basis</td><td colspan="2">Principle of autonomy/self-determination</td></tr>
<tr><td>Primo non nocere/do no harm/ principle of non-maleficence
Principle of beneficence</td><td>Right to privacy, to be treated with dignity and respect</td></tr>
<tr><td colspan="2">World Medical Association Declaration of Helsinki (2013)</td></tr>
<tr><td>Legal and regulatory basis</td><td>National implementations of:
International ethical guidelines for health-related research involving humans, published by the
Council for International Organizations of Medical Sciences (CIOMS) in collaboration with the WHO (2016)
European Clinical Trials Regulation[a]</td><td>GDPR and one of the bases from Art. 6 in conjunction with Art. 9 for special categories of data (including national implementation of selected bases from Art. 6 and exemptions from Art 9)
Implementations of:
GDPR Art9(4) GDPR
The US Health Insurance Portability and Accountability Act 2016 (HIPAA)
EU Charter of Fundamental Rights (Art. 8)</td></tr>
<tr><td colspan="3">[a] The Regulation and its Articles 28 and 29, concerning informed consent, apply directly and do not require national implementation.</td></tr>
</table>

Medical research guidelines have, as their main focus, protection from risk of harm, and have gradually grown to encompass and overlap with oversight over data protection. This blurring of lines is well reflected in the overlap of institutional duties of ethical review boards and data protection agencies in some countries. At the same time, there is an inevitable and dynamic blurring of the distinction between

ethics and law. There are acts and arrangements that are legal but unethical and similarly, more importantly, laws should ideally be based on sound ethical principles, but the distinction is dynamic in time. The distinction between the legal and the ethical basis for informed consent also illustrates the two uses of the concept – namely as either solely an administrative tool to document compliance with legal-regulatory obligations or, in addition, an ethical practice and procedure to support and reinforce patient autonomy.

Although the bulk of this guide relates to consent relating to personal data collection and use, this section begins with a summary of the ethical basis of consent.

5.1.2 Ethical bases for consent

Different professional associations, organisations, agencies and universities have adopted rules and policies outlining ethical principles and requirements. For the purpose of this guidance, ethical consent is based on the ethical standards set forth in the Declaration of Helsinki issued by the World Medical Association (WMA). Although this declaration is not legally binding, it is an internationally recognized standard for medical research involving human subjects, including research on identifiable human material and data. National legislation has been passed in nearly all European countries to reflect these standards.

The dominant focus of the Helsinki Declaration is to articulate the ethical principles that will protect humans involved in medical research against physical and mental harm. Informed consent is not an ethical value in and by itself but is an essential means to this end: protection against harm. More precisely, protection against unacceptable risk of harm, voluntary or not, in a context of risks, burdens and benefits to the patient and where, for some patients, the risk of harm of an experimental intervention can be outweighed by the certain progression of a more harmful disease. The other essential protection against harm is the requirement that no experimental trial involving humans can be undertaken unless approved by an ethical review board assessing the quality of the trial including its protections of subjects involved.

The earlier versions of the Helsinki Declaration were focused almost solely on protection against unacceptable risk of physical and mental harm. But the 5th revision from the year 2000, while describing in the introduction that the well-being of the individual subject takes precedence over the need to improve the common good of advancing medical science and know-how, also states that it includes "research on identifiable human material and data". The tasks of the ethical review boards have therefore gradually developed to include or overlap with overseeing that any proposed medical trial has submitted a satisfactory plan for managing personal data, i.e., that not only should the patient be protected against physical and mental harm, but also against what can be called moral harm, viz. violation of privacy. Ethical committees now therefore tend to consider data aspects, with the benefit of information governance input/representation. The review board should therefore ensure that the trial leaders have produced a legally and regulatorily compliant plan for the form, content and process of acquiring informed consent as well as data security.

The Declaration of Helsinki requires a consent for medical research studies. If researchers also use consent as a primary legal basis for processing personal data, two different consents should be obtained in order to conduct the study: a data protection consent and a consent compliant with ethical standards. In contrast to the GDPR, the Declaration of Helsinki does not provide a definition of "consent". However, paragraphs 25 to 32 set forth the requirements of the ethical-based informed consent. The patient should be adequately informed of the aims, methods, sources of funding, any possible conflicts of interest, institutional affiliations of the researcher, the anticipated benefits and potential risks of the study and the discomfort it can entail, post-study provisions and any other relevant aspects of the study.

Furthermore, the consent should be given voluntarily. In this regard, the Declaration of Helsinki specifically mentions that the researchers should take into consideration the dependent relationship of the potential subject with the physician. Although, the GDPR-based and the ethical-based consent have similar requirements, it is important to note that they have different objectives and backgrounds. From an ethical point of view, the consent is necessary to make sure that the patient makes a voluntary and

informed choice to take part in a study, whereas the consent in the sense of the GDPR ensure lawfulness of the processing of personal data. In practice, this is often confused. It is therefore strongly recommended to always treat them separately. This does not mean that it is impossible to seek consent that would satisfy both the GDPR's standards and relevant ethical standards at the same time, but it is important that participants understand the different consequences of these consents including the possibility to withdraw each consent separately or jointly at any time. Examples when (ethical) consent and GDPR and other data requirements diverge apart are provided by vaccination programmes for infectious diseases with severe population consequences. In some countries, immunization is mandatory, in others strongly recommended while schools can require it. Similar levels of COVID test or vaccination requirements have been implemented.

5.1.3 Legal and regulatory bases for consent

Within the countries committed to following the GDPR legislation there can be minor variation in instituted laws but also large variation in nomenclature and laws about personal data protection. Such variations will be even greater outside the GDPR committed sphere of countries. To this variation should be added that requirements to forms of consent will differ depending on whether they concern protection against harm from trials or against misuse of data.

GDPR transparency is also a key when it comes to the withdrawal of consent. Both legal and ethical consent, require that a data subject's consent can be withdrawn at any time, without necessarily negating the effect of the other. It is therefore important to clearly communicate to the data subject the consequences of each withdrawal. When drafting information for research participants, it can be relevant to take into account the stipulations of ISO 14155 – Clinical investigation of medical devices for human subjects – Good clinical practice (GCP) regarding withdrawal of consent for data use, if consent is being obtained for, or data are being reused from, regulated clinical trials.

When involving human subjects in studies, it is therefore key to communicate the difference between the GDPR consent requirements and the ethical consent obligation in a transparent way.

NOTE Ethics committee applications can require a categorical policy on the handling of ethical dilemmas such as information about a definite risk that has been identified through research (e.g., a genetic disposition for a disease that the patient can do something about it or where nothing can be done).

5.2 Consent as the basis for processing personal data within research

In the context of research which would aim to enable the use of the data in the future, for possibly not yet known research activities, it can be difficult to comply with the elements indicated, especially with the requirements of a specific and unambiguous consent, as the purpose for any further processing, an intrinsic part of consent, is unknown and cannot be specifically defined at the time of data collection. According to GDPR, Recital 33, in the context of processing of personal data for research, data subjects "should be allowed to give their consent to certain areas of scientific research". This implies that a more general consent will not be invalid for lack of particularity if provided in the context of scientific research. Nonetheless, the GDPR, Recital 33 continues to also state that "[d]ata subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects allowed by the intended purpose." Nevertheless, a broader approach to the consent would definitely allow for a more efficient use of already collected data for the needs of the future research activities (see 5.4). In addition, selected national legal acts, further defining conditions for processing of data concerning health for the research purposes, provide that the purposes to which a consent can be given could be defined at a more general level. Such an example is included in Article 3(1)(e) of the Irish Health Research Regulation, which states that explicit consent can be obtained from a data subject "for the purpose of the specified health research, either in relation to a particular area or more generally in that area or a related area of health research, or part thereof". This basis can be a favourable legal basis for prospective data processing in a research project, where consent can be obtained at the stage of data collection. According to the Preliminary Opinion 8/2020 on the European Health Data Space (15), 17 November, 2020 Art 6(1) GDPR cannot be the most appropriate legal basis to enhance access to health data. Instead, Art 6(1)(e)

GDPR can be the appropriate legal basis for the processing of personal data in the context of the functioning of the EHDS, as the platform's main purpose will be to serve the public interest and the processing should be done in the exercise of official authority vested in the data controller.

When it comes to processing of retrospective data, consent can be an appropriate legal basis only if the initial consent collected for the primary research was sufficiently broad to also include further research purposes. As an example of this, in Ireland Health Research Regulation 3(1)(e) provides that explicit consent from the individual can be obtained "for the purpose of the specified health research, either in relation to a particular area or more generally in that area or a related area of health research, or part thereof".

GDPR, Art 5 sets forth a number of basic principles when processing personal data. In order to process personal data a person or entity requires a legal basis [GDPR, Art 5 (1)(a)]. To fulfil this requirement, processing activities should be based on one of the legal bases under GDPR, Art 6. If the personal data being processed include health related or genetic information, as is usually the case in the context of health research, additional requirements should be met, as these data represent "special categories of personal data" [GDPR, Art 9(1)]. Processing of such types of data is generally prohibited by the GDPR, unless one of the exemptions defined in GDPR, Art 9(2) applies. In the context of processing special categories of data, processing based on consent has to fulfil the requirements of GDPR, Art 9(2)(a) – consent should be explicit, i.e., cannot be implied or tacit.

Therefore, researchers processing health related or genetic personal data should ensure they satisfy both one of the legal bases enunciated in GDPR, Art 6 in conjunction with one of the exceptions defined in GDPR, Art 9(2).

The data controllers processing the data can rely on a number of different legal bases defined in the GDPR:

a) consent of a data subject [GDPR, Art 6(1)(a)];

b) conclusion of a contract or fulfilment of the obligations set out in a contract concluded with the data subject [GDPR, Art 6(1)(b)];

c) compliance with a legal obligation to which data controller is subject [GDPR, Art 6(1)(c)];

d) protection of the vital interests of the data subject or of another natural person [GDPR, Art 6(1)(d)];

e) public interest [GDPR, Art 6(1)(e)];

f) legitimate interest pursued by the data controller or by a third party [GDPR, Art 6(1)(f)].

In the context of health research, the legal bases defined in points 1, 5 and 6 are the most relevant. These legal bases have been already considered and applied in R&I projects and will be further described in detail in the subsequent sections.

In the context of health research, the GDPR does not restrict the application of Art 6 only to consent. The legal bases which can be considered when processing special categories of data, alternative to consent, are usually GDPR, Art 6(1)(e) or (f) in conjunction with one of GDPR, Art 9(2)'s exemptions.

Considering all the above-described limitations of relying on consent as a valid legal basis for the processing of health related personal data, researchers can seek other legal bases for personal data processing, which would avoid the consequences of invalidity or withdrawal of consent.

5.3 Alternative legal bases for processing personal data

5.3.1 General

This guide focuses on consent as the most commonly used legal basis for processing personal data in the context of developing, piloting and evaluating a digital health innovation, or for other kinds of health related research. As indicated in the earlier sections, informed consent can in any case be required for ethical reasons, and so adding consent for data processing (in conformance with the GDPR) can be most appropriate. However, it is important to consider the other options that are specified in the GDPR as legal bases for processing personal data. These can be relevant if, for example, new processing is desired and the act of obtaining fresh consent for new processing is not practical.

The first alternative legal basis permits data processing as part of the performance of a task in the public interest. It is a suitable basis for medical research as stated by the European Data Protection Board and the European Data Protection Supervisor (EDPS) [GPDR, Art 6(1)(e)]. Nevertheless, to rely on this legal basis, a particular EU or Member State law should recognize the purpose of the processing as being in the public interest [GDPR, Art 6(3)].

The second alternative legal basis refers to the legitimate interest of the entity processing the data, but only if those interests prevail over the interests and fundamental rights and freedoms of the data subjects, taking into consideration the reasonable expectation of data subjects based on their relationship with the data controller. The determination of the existence of a legitimate interest needs a careful assessment "including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose can take place" (GDPR, Recital 47). Data processing for research purposes could constitute a legitimate interest, as it can be compelling and beneficial to society at large [GDPR, Art 6(1)(f)].

As stated in subclause 5.2, when processing health and genetic data, in addition to a legal basis under GDPR, Art 6, the entity or person processing personal data should identify an exception under GDPR, Art 9(2). Otherwise, the processing will be considered prohibited (GDPR, Art 9(1)). Considering the legal bases defined in GDPR, Art 6(1)(e) and GDPR, Art 6(1)(f), the most appropriate exceptions which can apply in conjunction with the mentioned bases and can allow for processing of data concerning health and genetic data are:

a) Substantial public interest: GDPR, Art 9(2)(g)

   Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which should be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

   In that regard, it is crucial to assess whether the reason for which the data controller processes special categories of data can be interpreted as "substantial public interest." This assessment will depend on the EU or national law applicable to the data controller.

   EXAMPLE 1 The conditions for substantial public interest are included in paragraphs 6 to 28 of Schedule 1, Part 2 of the UK Data Protection Act 2018 – an act implementing UK GDPR (the act mirroring the GDPR provisions). Among them there are: support for individuals with a particular disability or medical condition, or equality of opportunity for or treatment of people with different states of physical or mental health. Their applicability, however, has to be considered always on a case-by-case basis, based on the test introduced in the mentioned legislation.

b) Public interest: GDPR, Art 9(2)(i)

   Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of

health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

The data controller should be able to demonstrate the necessity of the processing for reasons of public interest in the area of public health. The term "public interest" is not defined, however, the data controller has to indicate a benefit to the broader public or society as a whole instead of pointing to his/her own interest. This exception might apply whenever processing is necessary for, e.g., improvement of healthcare provision (Opinion of the Data Ethics Commission), clinical trials of drugs or medical devices or responding to new threats to public health. Additionally, the public interest in the domain of public health can be further defined in the legal acts adopted either at the European Union or at national level. Therefore, it is important that the data controller who would like to base the processing of data concerning health on this exception is able to indicate what legal provision it is based on.

EXAMPLE 2 The Irish Data Protection Act 2018, Part 3, Chapter 2, Section 53 defines that the "public interest" reasons in the area of public health includes "protecting against serious cross-border threats to health" and "ensuring high standards of quality and safety of health care and of medicinal products and medical devices".

c) Scientific research and statistical purposes: GDPR, Art 9(2)(j)

For health research, the exemption which appears to be the most appropriate and can constitute a valid legal basis, can be found in GDPR, Art 9(2)(j), which permits processing of special categories of data for scientific research and statistical purposes in accordance with GDPR, Art 89(1), based on Union or Member State law. In other words, this exception can be relied upon only if data processing for mentioned purposes is envisaged by EU law or Member State law and if the safety and security measures, indicated in GDPR, Art 89(1), especially pseudonymisation measures, are implemented to safeguard fundamental interests of the data subject.

It should be further highlighted that EU countries can maintain or introduce further conditions on the processing of data concerning health and genetic data. This includes limitations, for processing of this type of data [GDPR, Art 9(4)]. Therefore, it is of utmost importance that entities processing data in a health research project check national regulations applicable to such processing and assess if, according to those national regulations, they are allowed to process the relevant data.

5.3.2 Scientific research and presumption of compatibility

The distinction between scientific research based on initial or secondary usage of personal (health) data is important in the context of the legal basis for the processing, and the purpose limitation principle pursuant to GDPR, Article 5(1)(b). According to the purpose limitation principle, personal data shall be "collected for specified, explicit and legitimate purposes". The general rule requires that in the case of further processing, if it does not fall within the initial purpose, the controller should perform a compatibility test (defined in GDPR, Article 6(4)). Nevertheless, GDPR, Article 5(1)(b) sets forth an exception and defines that further processing for scientific research purposes in principle should not be considered incompatible with the primary purposes for which the data were collected. This presumption can be applied only if an additional condition is fulfilled. Namely, the processing activity for scientific research purpose shall be performed in accordance with GDPR, Article 89(1), i.e., as already highlighted in point 5.3.1 c), it should be subject to appropriate safeguards for the rights and freedoms of the data subject. "Appropriate safeguards" mean technical and organisational measures applied to respect data minimisation principle, such as, inter alia, pseudonymisation but only under pre-condition that the scientific research purpose can be fulfilled in that manner (GDPR, Article 89(1)).

Following that, in principle, scientific research, including health research, is almost automatically compatible, but this exemption shall "not be read as providing an overall exception from the requirement of compatibility, and it is not intended as a general authorisation to further process data in all cases for historical, statistical or scientific purposes". It is still imperative to consider all circumstances when processing data subjects' personal data, as with any other type of data processing, to safeguard their rights, freedoms, and interests.

As stated by the EDPB, in the situation where a healthcare provider who collected health data from their patients would like to use those data for scientific research, it may rely on the presumption of compatible use, but is required to consider also GDPR, Article 9, as it could be that the exemption that the health care provider relied on for initial purpose does not cover the processing of the same data for the purpose of scientific research. The EDPB presents the following example picturing such a case: if an exemption in the law of one Member State allows the health care providers to process the health data exclusively to provide health care of medical treatments, for the secondary use they would need to base their processing on an exemption based on the EU or MS law for scientific research purposes, as required in GDPR, Article 9(2)(f).

Moreover, such processing for scientific research purposes can only be considered as "further processing", as per the definition of further processing and the information outlined in Recital 50 of the GDPR, if the data has been previously processed by the same controller for a specific purpose, and now the controller intends to process the same data for a new (scientific research) purpose. When a new, separate controller aims to process the data for scientific research purposes, this planned activity does not classify as further processing, but as processing for initial research purpose by a new controller. Such processing is subject to all applicable data protection requirements, including finding a legal basis for processing (GDPR, Article 6) as well as exemption for processing health data (GDPR, Article 9).

5.3.3 Clinical Trials Regulation and the General Data Protection Regulation

While the GDPR ensures the protection of individuals with regard to the processing of personal data and harmonised rules on the free movement of such data; the Clinical Trials Regulation (CTR) aims at ensuring a greater level of harmonisation of the rules for conducting clinical trials throughout the EU. Notably, it introduces an authorisation procedure based on a single submission via a single EU portal, an assessment procedure leading to a single decision, rules on the protection of individuals, and informed consent and GDPR transparency requirements.

It is recognised in many jurisdictions that the interplay between these two regulations can seem complicated with regard to the different processing activities that might be undertaken during a clinical trial and with data derived from a clinical trial. The European Data Protection Board (EDPB) issued a detailed opinion in January 2019, extracts of which are reproduced below because they can be relevant to users of this guide who are determining what kind of consent or other legal bases can be appropriate for their context.

Regarding the processing of operations purely related to research activities the main points are:

— The informed consent foreseen under the CTR should not be confused with the notion of consent as a legal ground for the processing of personal data under the GDPR.

— The obligation to obtain the informed consent of participants in a clinical trial is primarily a measure to ensure the protection of the right to human dignity and the right to integrity of individuals under Article 1 and 3 of the Charter of Fundamental Rights of the EU; it is not conceived as an instrument for data protection compliance.

— In order to assess whether the individual's explicit consent can be a valid legal basis for the processing of sensitive data in the course of a clinical trial, data controllers should duly take into account the Working Party 29 Guidelines on consent, and check if all the conditions for a valid consent can be met in the specific circumstances of that trial.

— Data controllers should pay particular attention to the condition of a “freely given” consent. As stated in the Working Party 29 Guidelines on consent, this element implies real choice and control for data subjects. Besides, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the data controller.

— Depending on the circumstances of the clinical trial, situations of imbalance of power between the sponsor/investigator and participants can occur. The CTR expressly addresses these risks and requires the investigator to take into account all relevant circumstances, in particular whether the potential subject belongs to an economically or socially disadvantaged group, or is in a situation of institutional or hierarchical dependency that could inappropriately influence her or his decision to participate.

— A clear situation of imbalance of powers between the participant and the sponsor/investigator will imply that the consent is not “freely given” in the meaning of the GDPR. As a matter of example, the EDPB considers that this will be the case when a participant is not in good health conditions, when participants belong to an economically or socially disadvantaged group or in any situation of institutional or hierarchical dependency. Therefore, and as explained in the Guidelines on consent of the Working Party 29, consent will not be the appropriate legal basis in most cases, and other legal bases than consent should be relied upon.

— Data controllers should conduct a particularly thorough assessment of the circumstances of the clinical trial before relying on individuals’ consent as a legal basis for the processing of personal data for the purposes of the research activities of that trial.

Regarding the secondary use of clinical trial data outside the clinical trial protocol for scientific purposes the following points have to be considered:

— The secondary use of data refers to situations where the sponsor can want to process the data of the clinical trial subject “outside the scope of the protocol”, but only – and “exclusively” – for scientific purposes. The CTR considers consent for this specific processing purpose should be sought from the data subject or his/her legally designated representative at the time of the request for informed consent for participation in the clinical trial.

— If a sponsor or an investigator would like to further use the personal data gathered for any other scientific purposes, other than the ones defined by the clinical trial protocol, it would require another specific legal ground than the one used for the primary purpose. The chosen legal basis can or cannot differ from the legal basis of the primary use.

— Article 5(1)(b) GDPR provides that where data is further processed for archiving purposes in the public interest, scientific, historical research or statistical purposes, these should a priori not be considered as incompatible with the initial purpose, provided that it occurs in accordance with the provisions of Article 89, which foresees specific adequate safeguards and derogations in these cases. Where that is the case, the data controller could be able, under certain conditions, to further process the data without the need for a new legal basis. The presumption of compatibility, subject to the conditions set forth in Article 89, should not be excluded, in all circumstances, for the secondary use of clinical trial data outside the clinical trial protocol for other scientific purposes.

— Scientific research making use of the data outside the protocol of the clinical trial should be conducted in compliance with all other relevant applicable provisions of data protection as stated under Article 28(2) CTR. Therefore, the data controller should not be deemed exempt from the other obligations under data protection law, for example with regard to fairness, lawfulness (i.e. in accordance with applicable EU and national law), necessity and proportionality, as well as data quality.

5.3.4 Clinical trials and clinical investigations

According to the EU Medical Device Regulation (MDR, Article 63) the following point have to be taken into account regarding clinical trials and clinical investigations:

— Informed consent should be written, dated and signed by the person performing the interview and by the subject. The informed consent should be documented. Adequate time should be given for the data subject to consider his or her decision to participate in the clinical investigation.

— Information given to the data subject should:

  a) enable the data subject to understand:

    i. the nature, objectives, benefits, implications, risks and inconveniences of the clinical investigations;

    ii. the data subject's rights and guarantees regarding his or her protection, in particular his or her right to refuse to participate in and the right to withdraw from the clinical investigation at any time without any resulting detriment and without having to provide any justification;

    iii. the conditions under which the clinical investigation is to be conducted, including the expected duration of the data subject's participation in the clinical investigation;

    iv. the possible treatment alternatives, including the follow-up measures if the participation of the data subject in the clinical investigation is discontinued.

  b) be kept comprehensive, concise, clear, relevant, and understandable to the data subject;

  c) be provided in a prior interview with a member of the investigating team who is appropriately qualified under national law;

  d) include the Union-wide unique single identification number of the clinical investigation and information about the availability of the clinical investigation results.

— The information should be prepared in writing and be available to the data subject.

— In the interview special attention should be paid to the information needs of specific patient populations and of individual data subjects, as well as to the methods used to give the information.

— In the interview it should be verified that the data subject has understood the information.

— The data subject should be informed that a clinical investigation report and a summary presented in terms understandable to the intended user will be made available in the electronic system on clinical investigations irrespective of the outcome of the clinical investigation, and should be informed, to the extent possible, when they have become available.

5.3.5 Member states' legislation regarding research with genetic data

The GDPR refers to genetic data but not genomic data. It provides a definition of genetic data under GDPR, Article 4(13) and again refers to genetic data as a special category of personal data under GDPR, Article 9. However, there is a certain level of uncertainty and disagreement as to whether genomic data are also covered by the definition of genetic data in the GDPR. The PHG Foundation, in a report issued in 2020, highlights the uncertainty about which data, resulting from what forms of analysis, fall within the GDPR definition. Noting this challenge, the report suggests that the genomics community should be proactive in developing appropriate standards for de-identification of genomic data through a code of conduct or

certification scheme setting out best practice for specific contexts and forms of data. This could help build consensus and achieve harmonization of national and international approaches under the GDPR given the potential that such a code or certification scheme can be formally recognised under the GDPR. When it comes to genetic data, the Oviedo Convention should also be observed. It entered into force in 1999, and in combination with its additional protocol concerning biomedical research, aims to provide a legally binding instrument to protect human rights with regards to biomedical data, including genetics and transplantation of organs and tissues. However, the convention only sets a minimum threshold of due notification and does not consider research making secondary use of biosamples and genetic data. In addition, the additional protocol concerning research was only ratified by six EU Member States (BG, CZ, HU, PT, SK, SV) and a total of 12 countries. As a result, and in line with Article 1 of the Oviedo Convention, room is left for national laws to provide regulation. With the introduction of the GDPR this has not fundamentally changed.

While the GDPR defines genetic data, it does not provide a harmonised regulatory context as with the rules governing the research; use of genetic data will in a large part be subject to national interpretation and already existing laws. The GDPR also does not govern as such the biological samples from which genetic and genomic data can potentially be derived. In this respect, GDPR, Article 9(4) allows Member States to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health, resulting in a situation where a few countries, such as France, Finland and Italy have specific provisions governing genetic research, whereas others do not.

In Member States where specific legislation for genetic research has been introduced, the legislation varies in its requirements. This ranges from an obligation to obtain explicit consent in Hungary, while in Spain under Law 14/2007 on Biomedical Research there is a legal requirement to notify data subjects about the possibility of finding unexpected results or results that can affect relatives. There is also an obligation under Spanish law to return results relevant to health and to provide genetic counselling; however, there is uncertainty as to the status of this law following the introduction of new data protection law. The Italian feedback indicated that pursuant to art. 2-septies of the Data Protection Code, the Italian DPA should adopt provisions outlining safeguarding measures with regard to the processing of genetic, biometric, and health-related data however, these safeguarding measures have yet to be issued by the Data Protection Authority (DPA).

5.4 Broad consent and data altruism

5.4.1 Broad consent

One of the most difficult challenges faced by clinical research when utilising consent as a legal basis for processing data is the obligation in the GDPR for the consent to be specific. This means that the purpose of processing needs to be narrow enough that it can be precisely explained and a data subject clearly understands why and how their personal data will be used if they give consent, by whom and with what safeguards. Research on the other hand often benefits from being able to use health data for multiple purposes, such as research questions and in research projects, that were not known at the time of obtaining consent. There is therefore a fundamental conflict between the requirement to seek specific permissions and the ideal scenario for research which is to have broad permissions. The concept of broad consent is not new and has been used with considerable variability across the world over many years.

It is universally agreed that progress and innovation in health research would be severely hampered if data from previous research and healthcare records were to be disallowed. Yet, the public interest in having health data available for research to benefit wider populations and future generations can easily clash with principles of informed consent. Several attempts to define a wider concept of informed consent are being made, not least in the context of European regulations. This is foreseen in EU Clinical Trials Regulation, Article 29 where the need for collecting “data from clinical trials to be used for future scientific research” is addressed. For such future use to be legitimate, it is stipulated, individuals should give their consent to use their data “outside the protocol of the clinical trial and [have] the right to withdraw that consent at any time”. It appears therefore that research can rely on some form of “broad

consent" that secures future and, at the time of consent, unspecified use of data for "medical, natural or social sciences research purposes".

An objection against any version of broad consent is that consent cannot possibly be both broad and informed. A broad consent is, by definition, consent to a future and, at the time of consent, yet unspecified use of data. However, how can informed consent be genuinely informed if the individual whose consent is sought does not know the purpose of the future use? Broad consent is therefore uninformed consent. Nevertheless, this objection can be met by ethical reflection on the basis for protection of privacy and autonomy on which requirements to informed consent are based. It will be argued that to respect citizens' autonomy and free choice is not possible if they are prevented from exercising their free choice of allowing their data to be used for future research. When individuals state that they are sufficiently informed about the range of possible and as yet unspecified purposes that their data can be used for, it would be an unethical restriction on their self-determination to prevent their exercising this freedom.

Broad consent can be characterised as a form of consent permitting individuals to collect data and samples for use in unspecified future research projects. The term has been given definitions by academics and organisations alike, which can be summarised by the data or sample subject being required to engage with the researcher or institute once. The legitimate use of broad consent has also been explicitly recognised in EU Member State law, as can be seen for example in Estonia and the UK.

However, with the introduction of the GDPR and the specific requirements that are enshrined within GDPR, Article 9(2)(a) for the processing and use of personal data that can be classified as sensitive on the legal basis of consent [as per Article 6(1)], the concept and use of 'broad consent' has become practically difficult and has, unsurprisingly, raised concerns that have been voiced in the genomic research community.

GDPR, Article 9(2)(a) clearly states that the processing of sensitive personal data in genomic research is possible if "the data subject has given explicit consent to the processing of those personal data for one or more specified purposes". This consent will only be legitimate however if it fulfils the conditions contained in GDPR, Article 4(11), which equates to 'consent' being freely given, specific, informed and unambiguous. To add to the problematic conditions which relate to the practical implication and need for specificity in the scope of consent, the Working Party 29 'Guidelines on consent under Regulation 2016/679' and further EDPB Guidance in the use of consent in health research do not provide clarifications and contain less favourable pronouncements on broad consent.

In light of the above, scientific research projects can only therefore in practice include personal data on the basis of consent if they have a well-described purpose, specific timelines and can require subsequent rolling granular consents.

However, a newer regulation, the EU Data Governance Act, is introducing a formal process whereby more flexible uses of data can be feasible whilst conforming to the GDPR.

5.4.2 Data Governance Act

5.4.2.1 General

One of the main objectives of the Digital Single Market strategy of the European Union is to provide a reliable and safe legal framework to enhance the free-flow of data. To encourage the sharing of data in the public interest, the proposal of the Data Governance Act by the European Commission introduces a new legal framework for "Data Altruism Organisations". Through these new rules on data altruism, the European Commission envisions that data "is made available without reward for purely non-commercial usage that benefits communities or society at large (…)." By certifying qualified organisations as a 'Data Altruism Organisation recognised in the EU', individuals and companies should be encouraged to share their data in the general interest. Based on the provisions on Data Altruism in the Digital Governance Act, the European Commission will adopt a common "European data altruism form".

NOTE In its current, non-final version, this act does not provide for commercial uses of data, which would exclude industry research such as drug, vaccine, device, algorithm development.

5.4.2.2 Data Altruism

The explanatory note given by the European Commission under the DGA policy explanation is that the concept of data altruism is meant to be taken as "individuals and companies giving their consent or permission to make available data that they generate – voluntarily and without reward – to be used in the public interest". This is also in line with the definition given under DGA, Article 2(16) as well as the voluntary sharing of data on the basis of consent given by data subjects for the common good, namely to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law, where applicable, such as healthcare.

Further, various statements and communications released by the European institutions such as the Commission Communication on a European strategy for data (COM/2020/66 final) refer to data altruism as an issue which will be addressed by the legislation foreseen on data spaces in order "to make it easier for individuals to allow the use of the data they generate for the public good, if they wish to do so ("data altruism"), in compliance with the GDPR."

It is noteworthy to mention that, in spite of the mirroring between the definitions provided by the institutions on what can constitute 'data altruism' and the seeming alignment that the definition has with prior uses the EDPB notes in its statement on the DGA (05/2021) the definition, among other terms, is not entirely consistent with the GDPR, notwithstanding the statement in the recital that it is "without prejudice" to the Regulation. It is therefore possible that there will be a period of uncertainty about the extent of flexibility that will exist for data altruism organisations to obtain GDPR conformant consent that contains some degree of broad consent permission.

5.4.2.3 Register of recognised data altruism organisations

In Chapter IV titled "Data Altruism", the Data Governance Act introduces a voluntary certification framework for non-profit organisations. Organisations that meet certain criteria specified in DGA, Art 16, can request to be entered in the register of recognised data altruism organisations. The European Commission intentionally chose a voluntary, rather than a compulsory, and low intensity regulatory approach in order to lower the administrative burden for organisations engaging in data altruism.

National authorities designated by each Member State will keep registers of recognized data altruism organisations [DGA, Art 17(1) - 19]. These authorities should meet certain impartiality and GDPR transparency requirements listed in DGA, Art 20.

The competent national authority in the Member State in which the entity has its establishment will exclusively handle applications for registration [DGA, Art 17(1)]. If an entity has establishments in more than one Member State, it should register in the Member State in which it has its main establishment [DGA, Art 17(2)]. In addition, the European Commission will maintain a Union register of recognised data altruism organisations [DGA, Art 17(2)].

Organisations should meet five requirements in order to qualify for registration as a data altruism organisation.

First, the organisation has to carry out data altruism activities [DGA, Art 18(a)].

Second, the organisation should be a legal entity constituted to meet objectives of general interest [DGA, Art 18(b)].

Third, the organisation should operate on a not-for-profit basis and be independent from any entity that operates on a for-profit basis [DGA, Art 1(c)].

Fourth, the organisation should perform the activities related to data altruism through a legally independent structure, functionally separate from other activities it has undertaken [DGA, Art 18(d)].

Fifth, the organisation should comply with the rulebook defined in the DGA, at least 18 months after the date of entry into force of the delegated acts referred to the rulebook [DGA, Art 18(e)].

6 Consent and novel digital health innovations

6.1 General

As technology in the health space continues to develop, novel digital health innovations are altering the methods of collecting, delivering and exchanging health data. In some cases, these data driven tools cannot change patient care, however they do have an impact on interactions between patients, healthcare organisations and personal data. This clause of the document provides guidance to innovators who apply consent as a legal basis for data processing when introducing a novel digital health tool.

When consent is relied on as a legal basis for processing, difficulties can arise as novel digital health innovations impact on the interactions between actors and involve complex processing operations. As a starting point, it is essential to determine the roles and responsibilities of each actor in a given processing operation based on GDPR definitions of data subject, data controller and data processor. This classification has a significant impact on the conditions for consent as a legal basis for processing and the responsibility to satisfy these conditions, and if/how robust data flows can be mapped between the pre- and post-deployment situations.

6.2 Consent requirements when introducing a novel digital health tool

6.2.1 Establish the data protection roles and responsibilities

6.2.1.1 General

When introducing novel digital health innovations, establishing the data protection roles and responsibilities could be challenging for a variety of reasons. Firstly, interactions between actors can be changed to the point that confusion arises with regards to the classification of data subject, data controller and data processors. In such instances, it can become difficult to identify which actor is responsible to satisfy GDPR conditions for consent. Secondly, some novel health solutions purport and aim to give citizens greater control over their health data. In such instances, the data subject can retain primary control over important processing activities such as the storage, exchange and erasure of their personal data. This can create uncertainties regarding accountability, the burden of enforcement and compliance. These challenges give rise to the following questions: who is responsible for satisfying the conditions for consent? Who is responsible for composing a suitable consent document, obtaining that consent in a proper way, and for managing and maintaining the documentation of that consent? How do these responsibilities and conditions for consent change when adopting a digital health innovation?

The concepts of data controller, joint data controller and data processor therefore need to be well understood and correctly applied to a project team or consortium. In the case of a research consortium, such as a European R&I project, it is essential to be clear and correct about which partners are acting as data controllers separately or joint, and which are data processors. These concepts are explained below.

6.2.1.2 Data controller(s)

The role of data controller does not stem from the type of entity but from the influence exerted over the processing of personal data. The word “determines” in the GDPR, Art 4(1) definition indicates that the data controller has the power to make decisions about key elements related to processing activities. This controllership can be imposed by law or established based on the facts of a processing activity. In some instances control can be inferred from legal provisions in national or Union law. Where controllership is established by law, the purpose of processing is determined by the law and the entity designated to achieve this purpose is the data controller. In most cases where control is not established by law, it is important to assess the circumstances surrounding the processing of personal data. In such instances, a

data controller is the actor which exerts influence over the purpose and means of processing personal data in a given processing activity.

The text of the GDPR indicates that the data controller should decide on both the purpose and the means of data processing. The purpose (the why) refers to the reason or objectives for the processing, why the processing is taking place (i.e., "to what end?" or "what for?"). The means (the how) refer to how these objectives should be achieved (i.e., "what measures should be employed to achieve the objectives"). The European Data Protection Board (EDPB) makes a distinction between essential and non-essential means. Essential means are reserved for the data controller and non-essential means for the data processor. Essential means are closely connected to the purpose and scope of the processing. Essential means can include which data is processed, who has access to the data and the duration of processing. It is not necessary that the data controller actually has access to the data being processed, the law is simply focused on who has a determinative influence on the purposes and essential means of processing.

In cases where one or more actors pursue a joint purpose using jointly defined means, this leads to a joint controllership. Parties in a joint controllership relationship should enter into a Joint Controller Agreement in accordance with GDPR, Art 26. The Joint Controllership Agreement determines the responsibilities, roles, and relationships of each data controller. The essence of the agreement should be provided to the data subjects. The agreement should contain the following information:

— details of the processing activities;

— the categories of personal data processed and the purposes of processing;

— the obligations and duties of each data controller with respect to their obligations under the GDPR, Art 26(1).

The responsibilities of each data controller with regards to giving effect to the rights of the data subject and their duty to provide information referred to in GDPR, Art 13 and 14.

The distinction between data controller and data processor is essential because in the context of consent, the data controller has specific responsibilities. The data controller has the responsibility of satisfying the conditions for consent and demonstrating that the data subject has consent to the processing of personal data.

6.2.1.3 Data processor(s)

Based on the GDPR, Art 4(8) definition, there are two basic requirements for classification as a data processor:

— The data processor is a separate entity in relation to the data controller(s);

— Personal data is processed on behalf of the data controller(s).

The data processor is a separate entity in the sense that the data controller decides to delegate processing activities to this external party. The data processor should act on behalf of the data controller(s) and under the direct instruction, authority or control of the data controller(s). The data processor(s) infringes the GDPR by acting beyond the purposes and instructions of the data controller. However, the data processor can determine the non-essential means of processing in order to achieve the purposes of the data controller. As such, in many cases the data processor determines the practical and technical aspects related to the implementation of processing, such as the hardware or software utilised in the processing activities.

GDPR, Art 28 requires that processing by a data processor be governed by a contract or a legal act under Union or Member State Law. In most cases, it is necessary for data controllers to conclude data processing agreements with data processors who act on their behalf. GDPR, Art 28(3) and the Commission Implementing Decision on standard contractual clauses between data controllers and data processors

provide guidance on the contents of such an agreement. The data processing agreement should stipulate the following provisions:

— a description of the processing activities including the categories of personal data and the purposes for processing;

— the obligations of the data processors including that data can only be processed based on the instructions of the data controller, unless otherwise required by law;

— confidentiality requirements that should be upheld by the data processor;

— the duration of the processing of personal data;

— specification of the technical and organisational measures which should be implemented by the data processor to ensure the security of personal data processing;

— requirements for the data processor assist the data controller by maintaining records of processing activities in order to prove compliance and make available information necessary to demonstrate compliance;

— requirements for the data processor to facilitate and contribute to audits and inspections conducted by the data controller or another controller mandated by the data controller;

— provisions governing the use or involvement of sub-processors;

— provisions governing the transfer of personal data to third countries or to an international organisation in accordance with;

— provisions related to deleting and returning personal data (including copies) to the data controller at the end of the prescribed period of personal data processing or as required by law.

6.2.2 How to satisfy the conditions for consent

6.2.2.1 General

Having identified the actors in a given processing operation, innovators can more easily determine which actor bears the responsibility of satisfying the conditions for consent. Where consent is relied on as the legal basis for processing, the GDPR places the duty on the data controller to satisfy the conditions for consent prior to the processing of personal data. These are mainly outlined in GDPR, Art 4(11), Art 9(2)(a) and Art 7. To be acceptable, including to ethics committees who need to approve planned research or pilot projects, the consent should visibly comply with GPDR obligations: to be freely given, to be specific and fully informed, and be captured through an unambiguous explicit statement or action. These three concepts are explained below.

6.2.2.2 Freely given consent

The GDPR mandates that data subjects give their consent ‘freely’, this requires “real choice and control”. To ensure this element of freedom, digital health innovators, when acting as data controllers, should ensure that data subjects are not compelled to consent, nor will they endure negative consequences if they choose not to consent or to withdraw their consent. There should be enough time to enable the person to consider the request; they should not be rushed, and thus can entail coming back after the initial explanation. The concept of freely given also includes the absence of any incentives or encouragement to provide consent, such as the implied assumption that clinical care will be superior, and there cannot be financial or non-financial incentives to provide consent, although a reimbursement of incurred costs is usually permitted.

When assessing whether consent is freely given, special attention should be paid to the provisions in GDPR, Art 7(4). Based on these provisions, data controllers should be cautious when a request for consent to personal data processing is bundled with the acceptance of a contract or terms and conditions. Such bundling is lawful only if the personal data processing is necessary for the performance of that contract or a service. Where the requirement of necessity is missing, the consent given is presumed to be not freely given.

In many cases, novel digital health innovations involve multiple processing operations for more multiple purposes. In such cases a blanket consent (for processing activities and purposes) would be insufficient. The EDPB encourages innovators to ensure that data subjects are free to choose which purposes and processing operations they accept. Based on the functionalities of the novel tool, several consent requests can be necessary. GDPR, Recital 42 further clarifies that consent is not freely given if the "procedure for obtaining consent does not allow data subjects to give separate consent for personal data processing operations respectively (i.e., only for some processing operations and not for others)." Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment. GDPR, Recital 32 further states consent should cover all processing activities carried out for the same purpose(s), however, when the processing has multiple purposes, consent should be given for all of them.

6.2.2.3 Specific consent

Specific consent means that the purposes of data use for which consent is requested should be clearly and precisely specified. To comply with the requirement of 'specific' consent, the innovator should apply the following elements as suggested by the EDPB, Consent Guidelines:

— purpose specification – innovators should apply the purpose limitation principle by determining the specific, explicit and legitimate purpose(s) for their intended processing activity. Furthermore, data subjects should be specifically informed about the intended purpose(s) and should always give consent for a specific processing purpose;

— granularity in consent requests – innovators who seek consent for various different purposes should provide separate opt-in or consent requests for each purpose. In this way, data subjects are free to give specific consent for specific purposes;

— separation of information – innovators should ensure that they provide specific information with each consent request. This information should include the data processed for each purpose.

6.2.2.4 Informed consent

Providing data subjects with information before seeking their consent is an essential aspect for valid consent. The GDPR outlines certain factors which are essential for data subjects to make a choice, the EDPB has identified the following information as important for obtaining valid consent:

— the identity of the data controllers(s);

— the purposes of processing for each processing operation for which consent is sought;

— the type of data to be processed, and how it is processed (which need to specify which country or countries will undertake the processing – this is important in the case of European project consortia who need to share data between partners and countries e.g., for AI algorithm development or for evaluations);

— the possibility to withdraw consent and the process to follow for withdrawal;

— where relevant, information regarding the use of automated decision-making in accordance with GDPR, Art 22(2)(c);

— risks associated with data transfers due to the absence of an adequacy decision and the appropriate safeguards in terms of GDPR, Art 46.

GDPR, Art 7(2) and GDPR, Recital 32 outline how information should be provided to data subjects. Information should be provided using the following guidelines:

— information can be presented in many ways, such as written, oral, audio or video messages;

— information should be provided using clear and plain language. Where possible, innovators should avoid using legal or technical jargon which the data subject cannot understand;

— information should be provided in an intelligible and easily accessible format;

— information should be delivered free of charge.

The duty to provide information to data subjects in the context of consent, coincides with the data subject's right to be informed in GDPR, Art 13 and 14. When personal data is collected directly from the data subject and when personal data is not obtained from the data subject, the data controller has the duty to provide information to the data subject. This Information is typically provided to data subjects through a privacy policy which is a public document explaining how personal data is processed and how data protection principles are applied.

Many initiatives that develop digital health innovations either intend to undertake Medical Device Regulation certification or wish to keep the option open for such a certification after the project if the research is successful and appears to be commercially viable. It is therefore in parallel important to comply with consent requirements under the MDR (see 5.3.3).

6.2.2.5 Unambiguous indication of wish

The GDPR states that valid consent requires an "unambiguous indication through a statement or a clear affirmative action". The criteria of "unambiguous" means that requests for consent should be separate and distinct from other requests such as requests to accept terms and conditions. A "clear affirmative act" requires that the data subject should take an intentional action to consent to the processing of their personal data. Therefore, the GDPR recluses data controllers from offering per-ticked check boxes or opt-out boxes. This clear affirmative act should be indicated through a "statement". The statement can be presented in various forms written or oral. However, the EDPB notes that silence, taking no action or making use of a product or service cannot be regarded as an active indication of choice.

6.3 Consent for data reuse and data sharing

The data collected by patients and healthy individuals through the use of digital health innovations (to manage a health condition or to prevent one) can be invaluable for research. The research can be to further refine an innovative solution or might be to establish a wider evidence base for its value or might be in related or unrelated disease areas. It should not be forgotten that usually disease research needs control patients (e.g. subjects who don't have the disease or subjects who are not provided with a given treatment or digital technology), and that therefore all of the data collected through health systems and healthcare could have wider value than the original context of its capture. A historic challenge with enabling that reuse is that consent forms have often specified quite precisely the nature of a particular research initiative, the hypothesis it is trying to examine, the organisation or teams that will process the data and sometimes even specifying the country or countries.

It is important to note that personal data collected for healthcare cannot automatically be used in research without explicit (usually new) consent. This might apply, for example, to the data collected from a deployed digital health innovation that is primarily being used for care delivery but where there is a wish in parallel to conduct research to evidence the value of the innovation, to improve it, or to use the technology as a source of data for other research. Consent might need to cover the reuse of data from one

research project to future research projects that are either an extension of the original project or that are in the same general area of research.

The downstream reuse of collected data could include research that might not be anticipated at the time the consent was obtained, and possibly involve sharing the data with parties and countries that were not anticipated. This is a challenging but commonly occurring issue as it is very hard to identify all potentially useful future data uses at the time of obtaining consent.

The opportunity for the data to have a wider reuse potential is sometimes overlooked at the time of developing the consent procedure and forms but can be difficult to incorporate retrospectively. It is therefore vital to consider the opportunities for data reuse as well as for data sharing (within an existing research consortium and future research collaborations that can involve different partners and might extend beyond Europe) at the outset. Even if future uses cannot be explicitly specified, participants can sometimes be informed of (and consent to) a broad scope of potential reuses (for example, areas of health or kinds of health innovation).

In jurisdictions where it is permitted to use data collected for one purpose for a new purpose, before any access is granted it might be necessary to compare the two purposes (the original consented or otherwise authorized purpose and the new intended purpose for which the access request or disclosure is made) in order to decide if the new use is permitted.

It is important to state the conditions under which access to the data can be granted to others e.g., sensitive data might be safely shared through mediated/controlled access, specific user agreements can be signed, de-identification techniques, and/or case by case custom approval by the original research team. In some cases, it can also be appropriate to provide an opportunity for participants to select whom they agree to share their data with (and with whom they do not).

Consent forms and GDPR transparency notices should make clear that organisations seeking consent (presumably, the data controller or one of the joint data controllers) have an obligation to protect the data, to protect the confidentiality of the data subject, to only use the data and share the data in accordance with clearly specified intentions. If an anonymised version of the personal data will be created and used for a wider range of purposes, then a patient friendly explanation of how this anonymisation will be undertaken should be included. If the data will be held for a limited time period in a personally identifiable form, then the duration of this time period should also be provided.

If appropriate, consent forms should address the possibility of sharing data with other organisations and with other countries, future data publication (including storage in an open data repository) and/or the long-term retention of data for reproducibility.

The consent form wording should make clear if the individual has explicitly consented to a proposed or possible transfer of data outside the EU after having been provided with all necessary information about the risks associated with the transfer.

It is important that the terms of the consent obtained for the records within a dataset are tightly coupled to the data, so that if the dataset is shared with other parties in the future there is transparency to all future users about the terms of the consent and therefore any limitations on its use and future propagation that apply.

7 Obtaining consent

7.1 What would digital health innovators seek consent for?

There are several reasons why digital health innovators acting as data controllers require consent to collect and use personal health data. These include baseline information to better understand the disease, treatment effectiveness, health needs etc. that could evidence the case as to why the innovation is needed, engagement with potential future users of the innovation to formally capture requirements, to evaluate prototypes in vitro (for example by testing out the innovation that has been populated with dummy data)

or in vivo (for patients to test the innovation using their own health and care trajectory with or without the intention to rely upon any advice generated by the innovation), to collect data in a more formalised way through a clinical trial or large-scale evaluation in order to accumulate evidence of effectiveness and/or safety and/or benefit, or other usability and acceptability evaluation data for certification or other approvals and reimbursement purposes.

Informed consent is required for participation in all clinical investigations except under limited circumstances involving certain life-threatening situations, military operations, or public health emergencies. Furthermore, in those cases where it is impracticable to obtain consent (for example, where the research involves only excerpting data from subjects' records), when the research does not infringe the principle of self-determination and does not create any risk for the included subjects (for example, retrospective studies), and finally when it is of high clinical importance for the general good, the responsible ethical committee can waive some or all of the elements of informed consent. In all other cases, informed consent is needed.

Anonymization of data can be challenging, or even impossible; even significantly anonymized datasets are unlikely to satisfy the modern standards for anonymization set forth by GDPR and seriously challenge the privacy of participants. On the other hand, anonymization of personal data can challenge participant's data ownership. Withdrawal from the study can need elimination of all relevant personal data. This would be practically impossible in a truly anonymized dataset, to which the GDPR (and therefore the right to erasure of the data) would not apply. Informed consent should include this transparency (i.e. that withdrawal of consent and the request for erasure of personal data might not include the possibility of erasing anonymized copies of their data), and thus allow participants to fully estimate the value of their participation versus their data sharing.

Clinical investigations involving collection of human genetic material, biological samples and personal data challenge the established norms of informed consent. To start with, the biological materials are not in themselves data, subjects to data protection legislation, but the action of extracting information from the samples is deemed to be equivalent to the collection of personal data, at which point data protection legislation applies.

In the case of collecting human genetic and biologic material, most research projects present specific challenges when it comes to educate their recruited participants. Details of storage and broad sharing of biospecimens and data make it very difficult to describe in detail legal and ethical requirements of informed consent for all future uses. This can be impossible to cover since future research implications or risks related to the collected data are hard to be foreseen. To a large extent, the most heated controversy concerns the use of existing samples collected over years or decades for new research projects and not samples collected prospectively for research purposes. Several approaches (opt-in or opt-out) have been suggested previously and have been adopted by research institutions.

7.2 When is explicit consent required?

In some instances, processing of personal data could result in serious data protection risks and therefore explicit consent for such processing is required. Obtaining the explicit consent of data subjects is mandatory in three specific circumstances:

a) When processing special categories of personal data which reveal racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership. Special categories of personal data also include genetic data, biometric data, data concerning health, data concerning sex life and sexual orientation. According to GDPR, Art 9(1), the processing of special categories of personal data is prohibited except where certain grounds for processing are applicable. The explicit consent of the data subject is one of the grounds which justifies the processing of special categories of personal data.

b) The transfer of personal data to third countries (countries outside of the European Union) and to international organisations is strictly controlled under the GDPR. The basic rule is that international transfers are permitted on the basis of an adequacy decision made by the Commission or when the

data controller and data processor have provided appropriate safeguards to protect the rights and freedoms of data subjects. GDPR, Art 49 outlines some exceptions to this rule. In specific situations (in the absence of an adequacy decision, or of appropriate safeguards) internal transfers can take place when the data subject has explicitly consented to the transfer, having been informed of the potential risks.

c) Chapter 3 of the GDPR outlines the rights of the data subject, one of these is the right not to be subject to a decision based solely on automated processing, including profiling in accordance with GDPR, Art 22. This right aims to protect data subjects from the legal effects which arise from solely automated decision making. However, this right is not absolute and does not apply in certain specific circumstances including when based on the data subject's explicit consent.

Explicit consent is not vastly different from the standard consent previously discussed. The term "explicit" is connected to the way in which consent is expressed and requires a clearly affirmed statement by the data subject. Explicit consent should be communicated in words (written or oral). The EDPB suggests that explicit consent be collected through written statements because it can be difficult for data controllers to prove explicit consent through recorded oral statements. The following methods can be implemented to ensure that consent is explicit:

— Allow data subjects to issue written statements of explicit consent by filling in an electronic form, sending an email or uploading a scanned document containing their signature, or by using an electronic signature.

— Include an explicit consent request on websites and applications with text that clearly indicates the consent.

EXAMPLE 1 The EDPB suggests the following text: "I, hereby consent to the processing of my data".

— Implement methods that support two stage verification of consent.

EXAMPLE 2 The data subject can click a check box on a website and thereafter receive an email from the data controller notifying them of the intended processing. The data controller then asks for a reply email of agreement or requires the data subject to click a consent link.

7.3 What are the additional requirements for valid consent?

When consent is relied on as a legal basis for processing, the GDPR places additional requirements on the data controller(s) in order to ensure valid consent.

GDPR, Art 7(1) places an obligation on data controllers to demonstrate a data subject's consent. This requirement is further reiterated in GDPR, Recital 42 which states: "where processing is based on the data subject's consent, the data controller should be able to demonstrate that the data subject has given consent to the processing operation". Innovators have the freedom to implement technical and organisational methods to comply with the duty to demonstrate consent. However, this duty should not result in excessive amounts of additional data processing or the collection of any more information than is necessary. In order to appropriately demonstrate a data subject's consent, data controllers should implement the following guidelines:

— keep a record of consent statements, how and when consent was obtained;

— keep a record of the information provided to the data subject;

— maintain a record of operational and technical workflows/data flows to show compliance with the criteria for valid consent.

The withdrawal of consent is an additional requirement for valid consent. GDPR, Art 7(3) places an obligation on data controller(s) to ensure that consent can be withdrawn as easily as it is given at any time.

EXAMPLE If consent is obtained through only one mouse click, swipe or keystroke, then a similar method should be implemented for the withdrawal of consent.

This obligation essentially means that the withdrawal of consent should require undue effort by the data subject. When consent is obtained through electronic means, data controllers should adhere to the following guideline:

— data subjects should be notified of their right to withdraw consent at any time. This information should be provided before consent is obtained;

— data subject(s) should be informed on how to exercise the right of withdrawal;

— if consent is obtained through a service-specific user interface (via a website, app or email), the data subject should be able to withdraw consent via the same electronic interface;

— the withdrawal of consent should be as easy as it was to provide it, and at no financial cost to the data subject(s);

— the withdrawal of consent should not lower the service levels.

When consent is withdrawn, data processing which took place prior to the withdrawal remains lawful (in cases where the conditions for valid consent were satisfied). However, once consent is withdrawn, continued processing on this legal basis is unlawful. All processing operations should stop unless there is another lawful basis to justify the continued processing of data.

7.4 What not to seek consent for

When the research of interest provides significant clinical relevance, it does not involve more than minimal risk for the participating subjects, it does not infringe the principle of self-determination and the requirement of individual informed consent can obstruct completely the conduct of the research, the responsible ethical review committee can waive some or all of the elements of informed consent.

7.5 The process of collecting consent – good practices

The process of collecting consent also needs to be considered carefully. This means that the persons charged with informing data subjects and collecting their consent need the relevant skills including the ability to explain the requested processing in language that is suitable for the data subject to understand, to listen to and respond honestly and completely to any concerns or questions raised. The environment needs to be friendly and calm, and the consent experience should not seem to be rushed or pressurised. Coercion should always be avoided.

It is crucial to understand that developing and obtaining consent through an ICF should not be a one-time-process. Researchers (in their role as data controllers) should be ready to return to informing (or re-informing) their data subjects on the different aspects of the study in order to ensure their full understanding of the nature of their participation and that they are still willing to participate. Many research teams tend to involve participants even more, showing them the data to be collected (heatmaps) and decide together if all or part of it will be accessed or reused and thus enhancing their sense of data co-ownership.

Moreover, it should be clear to everyone (research team, sponsor, participant) that the study protocol can change if new scientific evidence occurs during its implementation period change.

Coercion and undue influence should always be avoided, in all cases and especially when the nature of the study involves provision of expensive medication or devices.

The length and complexity of the text presented and explained to the data subject in order to adequately inform about the terms of the consent need to be the minimum necessary to achieve adequate informing. No absolute guidance can be given on what length of explanatory material is appropriate for any particular consent process, but it is important to remember that over-elaboration carries the risk of confusing or demotivating data subjects, in terms of fully understanding the benefits, risks and purpose of their participation to the project.

In case of multicentric/multinational studies the ICF should be adapted to national legislation/ regulations (e.g. the EU Clinical Trials Regulation, the EU Medical Device Regulation) and be approved by local authorities in each case, without changing the scientific value of core clinical protocol.

GDPR, Art 4 stipulates that consent of the data subject should be:

— freely given: see 6.2.2.2;

— specific: see 6.2.2.3;

— informed: see 6.2.2.4;

— unambiguous: see 6.2.2.5.

Good practices to consider when obtaining consent:

— consent should be separate from other terms and conditions (‘unbundled’);

— pre-ticked opt-in boxes should not be used: choices should be expressly made by the data subject;

— separate consent is required for separate processing operations (‘granular’);

— each party relying on the consent should be clearly identified (‘named’);

EXAMPLE It is the view of the UK Information Commissioner’s Office (ICO) that “even precisely defined categories of third-party organisations” are not sufficient.

— consent needs to be documented: organisations need to record what an individual was told, what the individual consented to and when/how consent was given;

— consent should be ‘easy to withdraw’: it should be as easy for an individual to withdraw consent, as it was for them to give, and individuals need to be told that they have the right to withdraw consent, without being required to justify that decision, and how to do so - typically to enforce the message that by not consenting there is no adverse consequence;

— organisations cannot rely upon consent where there is a clear imbalance of power between the individual and organisation, as it is unlikely that the individual’s consent was ‘freely’ given in all the circumstances of that specific situation.

Table 2 below provides a summary of and checklist for valid consent which can be adopted by innovators as a guideline to follow when introducing novel digital health innovations.

Table 2 — Checklist for valid consent

Consent Elements	Requirements	Checkbox
Freely Given	Data subjects have real choice and control.	
	Data subjects are not coerced or compelled to consent.	
	Data subjects do not face negative consequences if they choose not to consent.	
	There are separate consent requests for different processing operations with different purposes.	
	The consent request is not bundled with the acceptance of a contract or T&Cs unless the processing of personal data is necessary for the performance of that contract.	
Specific	Specify the purposes for processing.	
	Ensure granularity of consent requests.	
	Provide specific information with each consent request.	
Informed	Provide important information to the data subject prior to obtaining consent.	
	Use clear and plain language, avoiding legal and technical jargon where possible.	
	Provide information in a clear and easily accessible manner.	
	Information should be provided free of charge.	
Unambiguous indication	Consent request for personal data processing should be separate and distinct from other requests.	
	Data subject should make an intentional and affirmative act to consent.	
	Silence or taking no action does not indicate choice.	
Capable of being withdrawn	Notify the data subject of their right to withdraw consent in the consent request.	
	Inform the data subject of the procedure to follow when withdrawing consent.	
	Data subject should be allowed to withdraw consent at any time.	
	Withdrawal of consent should not require undue effort by the data subject.	
	The method for obtaining and withdrawing consent should be equally as easy.	
Explicit	When consent is relied on as a legal ground for processing special categories of personal data, it should be explicit consent.	
	In the absence of an adequacy decision, or of appropriate safeguards, international data transfers can take place when the data subject gives their explicit consent.	

Consent Elements	Requirements	Checkbox
	Data subject can explicitly consent to be subject to a decision based solely on automated processing, including profiling.	
	Explicit consent requires a clear affirmed statement by the data subject.	
Demonstrable	Data controller has an obligation to prove that valid consent has been obtained.	
	Maintain records of consent statements, information provided to data subject and data flows to prove compliance.	
	When maintaining records, do not process an excessive amount of additional data or any more information that is necessary.	

7.6 Information security safeguards

Security of personal data is among the fundamental principles expressed within the GDPR, Art 5, with specific reference to its universally recognized pillars of confidentiality, integrity and availability. This principle is applicable to consent, considering the specified need for the data controller to demonstrate that the data subject has consented to processing of his or her personal data which implies a personal data processing for registering the consent and for maintaining it over time. Information security addresses the protection of confidentiality, integrity, availability by mitigating unauthorised access, processing, manipulation, loss, destruction and damage.

NOTE The European Union Agency for Cybersecurity (ENISA) has mapped the information security principle to the following clauses from GDPR, Art 5(1)(d) “accuracy”, Art 5(1)(f) “integrity”, Art 32 “Security of processing”, and Art 54(2) “Professional secrecy”.

Another relevant principle from GDPR where information security comes into play is the data protection by design and by default expressed in GDPR, Art 25. A key factor to ensure information security by design and by default is to identify information security risks before processing and apply an appropriate set of information security measures, among which one of the most relevant is the trust model. The trust model defines who needs to talk to whom and what type of traffic should be exchanged; all other information exchanges would be denied. Once the appropriate trust model is identified, the security measures that enforce the model can be defined. By performing a risk assessment of the potential threats presented by the processing, and through penetration testing, the requirement for additional security measures can be identified.

Within the sphere of information systems’ security, trust models are defined with respect to data providers’ relations and interactions with other involved actors in: trusted model, if sensitive data protection is the responsibility of a third party; untrusted model when data providers keep the responsibility of data protection; semi-trusted model when trust is distributed among the set of entities, involved in the execution of the protocols. Different lists of common information measures are available and can be used within this context, most notably within ISO/IEC 27701 and ENISA’s Handbook on Security of Personal Data Processing.

Among those measures, privacy enhancing technologies (PETs) are among the most relevant and include all the techniques consisting of information and communication technology (ICT) measures, products, or services that protect data by eliminating or reducing personal data or by preventing their unnecessary and/or undesired processing, all without losing the functionality of the ICT system.

It is beyond the scope of this guide to list or explain the information security safeguards that should be adopted, given the very diverse deployment contacts and data uses that different digital innovation initiatives might entail.

The main information security safeguards should however be outlined in the GDPR transparency notice, with consideration to use explanation and diagrammatic depiction of the intended data flows, storage locations and parties who will access the data at different points along these data flows. This needs to be clear enough that it provides the appropriate level of confidence and understandable enough for the intended majority of data subjects, with access to a person and/or to a glossary of terms to assist in its interpretation.

7.7 Consent from vulnerable patients

7.7.1 General

Informed consent implies that data subjects understand the data processing about which their permission is being sought, the choices they have available and the implications of those choices and importantly that there is no coercion impinging upon their free choice. It can be difficult to achieve this for vulnerable persons, for example children, persons with severe disabilities or mental health or educational challenges, persons with very severe diseases with limited hope for the future, disadvantaged or minority groups etc.

People's vulnerability is defined as a complex social phenomenon that both influences, and is influenced by, a range of processes and risk factors that can lead to or result from poor health:

— personal factors (e.g., biological, inborn, or acquired);

— external factors (e.g., social determinants of health).

People that experience restricted access to essential social, economic, political, and environmental resources, or limitations due to illness or disability are at higher risk of vulnerability. In contrast, the more personal resources and the stronger environmental support one has, the less prone to vulnerability one is.

In the International Convention on the Rights of Persons with Disabilities (New York Convention), the freedom of decision of persons with disabilities is granted (Art 3, 12, 14, 23 and 25). These articles include the right to make decisions freely about their lives, their care, medical treatment, and privacy. This includes: deciding on the treatment administered, deciding on daily aspects of their lives (where to live and with whom, having a partner, working, etc.), not being subject to arbitrary and total incapacitation, promoting less invasive measures of decision support. Within this freedom of decision, the consent of the interested party could be included. As the convention is inclined to "accompany" in decision-making, this should also be reflected when granting consent for the treatment of health data. As this aspect is not included in the GPDR, it should be harmonized at European level. In order to enforce valid consent forms for fragile adults, harmonization procedures for representatives' consent should be in place. In other words, a support system needs to be harmonized at European level for allowing vulnerable people to grant the consent for the processing of health data with the support they need.

What happens with the consent of the person with a disability, if they can grant it themselves or if it will be granted through representation. For example, in cognitively impaired older adults who cannot have the ability to give a valid consent, but there is an urgent need to use their data to improve eHealth and eCare innovative systems for meeting their needs regarding chronic diseases monitoring and other conditions. With regard to minors the MDR states that those who are capable of forming an opinion and assessing the information given to them, should also assent in order to participate in a clinical investigation.

NOTE Each Member State has introduced a different age by which minors can give consent for the processing of their personal data. For instance, Spain established that the processing of personal data of a minor age can only be based on her or his consent when she or he is over 14 years old. In case of minors under 14 years of age, the decision is in the hands of their legal representatives.

Data processing envisaged under the consent-form should take into account that consent is a suitable legal basis of the GDPR. The GDPR does not specifically refer to adult vulnerable people or those with disabilities. However, it is important that any digital health innovation or other research initiatives that involve collecting data from vulnerable people or is targeted for use by vulnerable people does recognise the importance of investing in appropriate means to engage with those persons and to obtain consent lawfully. This might involve having resources for caregiver and family assistance, the production of materials that are ability-appropriate, and conducting in person rather than remote methods of communication.

According to the MDR a legally designated representative can consent after having been duly informed when the data subject is not able to give informed consent. Where the data subject is unable to write, consent can be given and recorded through appropriate alternative means in the presence of at least one impartial witness. In that case, the witness should sign and date the informed consent document. The data subject or, where the data subject is not able to give informed consent, his or her legally designated representative should be provided with a copy of the document or the record, as appropriate, by which informed consent has been given.

7.7.2 Preventing prejudice against vulnerable populations

Data sharing in large-scale data processing projects needs to take into account the sources of information to avoid biases, especially concerning vulnerable populations that are not able to consent, and thus not to be represented due to lack of visibility in this kind of studies. Inequities can be exacerbated by regional inequities in data generation[1], from technical coverage to systematic biases in data collection should be taken into account. The following points should be observed when obtaining consent from vulnerable patients:

— the equity principle is not only for users, but also for data-sourcing (FAIR principles should include this aspect);

— guidelines for integrative data sources should be in place;

— making sampling, standardization, and sharing strategies transparent, could allow better integration of vulnerable population and communities' data. Moreover, whenever possible, the results of such assessments, as a trust and transparency-enhancing measure, should be made public by the data sharing service provider as well as by the user(s);

— data science often needs interoperability and centralized infrastructure, but it should be compatible with FAIR data generation decentralized strategies.

7.8 Avoiding coercion

Consent to participate to research should be entirely voluntary. Undue influence could occur when trying to obtain consent through an offer of an excessive, or improper reward or other kind of overture e.g., access to better healthcare. During the whole informed consent procedure, any intentional or unintentional action that can create coercion or undue influence should always be avoided.

8 Withdrawal of consent

Consent plays a significant role in terms of autonomous decision-making of the data subjects. It is at their discretion to decide for what purposes their data can be processed. Moreover, they can withdraw their consent at any time, in which case the processing should cease unless there is a new consent or a new legal basis. Considering that consents can stem from different obligations, such as GDPR and Declaration of Helsinki, it should be possible to withdraw the ethical consent without withdrawing the GDPR-based

[1] This has been the case in the COVID-19 pandemic data sharing strategies.

consent. This does not necessarily lead to an unethical processing, as long as the data subject understands the effects of the withdrawal. By withdrawing the ethical consent, participants of the study only wish no longer to actively participate in the research study. However, the processing of personal data could be still possible, if the data subject is informed about ongoing processing activities. In case of doubt, a data controller should consider both consents as withdrawn. A way to ensure full transparency could be to provide different options of withdrawal such as "no contact and use of my data", "no contact but you can still use my data".

The data controller should inform the data subject of this right before providing consent, and in so far as the data subject does not already have the information. The consent should be as easy to withdraw as to provide.

The qualifications for valid withdrawal at the GDPR are the following:

— withdrawal of consent does not affect the lawfulness of the processing that was based on consent before the withdrawal;

— if the data controller has another legitimate ground for processing personal data, the withdrawal does not lead to the end of the data processing[2]. In such cases, the data subject has still to be notified about the change in the lawful basis for data processing;

— the data controller is not obliged to delete data, unless there is no other legal ground for "retaining" data.

Withdrawal refers to consent that has already been given by the data subject, while objection is applicable to data processing that is not based on the consent of the data subject, but relies on GDPR, Art 6(1)(e) or (f) –limits in 21(1) - or involves direct marketing (GDPR, Art 21(2).

MDR, Art 62.5. 5 states that any subject, or, where the subject is not able to give informed consent, his or her legally designated representative, can, without any resulting detriment and without having to provide any justification, withdraw from the clinical investigation at any time by revoking his or her informed consent. Without prejudice to Directive 95/46/EC, the withdrawal of the informed consent does not need to affect the activities already carried out and the use of data obtained based on informed consent before its withdrawal.

9 Informed Consent Form

9.1 General

Three elements should be the core of the Informed Consent procedure, the Informed Consent Form (ICF) and the GDPR transparency notice (Information Sheet) [Jacob et all, 2011]:

— information: ensuring that the data subject receives full disclosure of relevant information;

— comprehension: ensuring that the data subject understands what is being asked of them;

— voluntary participation: ensuring that the data subject acts voluntarily in consenting.

9.2 Points to include in a GDPR transparency notice

a) Scope of the project and the role of the data subject's participation in it:

[2] Secondary use of health data for research does qualify

Purpose, duration, how many will be recruited, required procedures (including randomisation, if applicable), the fact that it is research (not individualised medical treatment) and key contacts.

b) Why the subject has been deemed suitable to include (e.g., how the eligibility criteria were met).

c) Types of data being collected and processed:

A clear but not detailed data management plan should be provided here, as well, showing that FAIR and data protection principles are respected.

d) Duration of data storage.

e) Data sharing with third parties, as intended in the study being performed and possibly to refer to future reuses of the data if the intent can be expressed specifically enough to be accepted:

The Open Access policy of a study should be also discussed here, if applicable.

f) Any data transfer outside the EU:

If affirmative, the conditions under which this will happen and the security measures taken should be described.

g) Data subject's rights:

It should be clear that participants can always ask the research team for additional information throughout the study, that if they change their mind about participating, they can leave the study and are under no obligation to explain why they are leaving, what the benefits and risks involved in taking part are and, what the costs involved or the compensations that can be provided are.

h) Risks and benefits from participating in the project.

i) If any costs incurred by the subject in participating in the research will be reimbursed (such as transportation costs to attend a trial centre, such as expectations that the subject will have or purchase a suitably specified smart phone).

j) How the study protocol could change if new scientific evidence occurs during its implementation period.

9.3 Points to include in the Informed Consent Form

a) Information about the project:

Brief and focused overview of the project, its background and objectives.

b) Who approved the study's protocol?

Identification of the Ethics Committee, Scientific Board Committee or other responsible authority. Dates and other details of the approval decision ensure transparency and will help towards the verification of the study's approval or the follow-up on possible amendments that can occur in the future.

c) Project participation – participant's workflow:

All procedures and timelines that concern the participant's involvement in the study, from their entry until the end of the study, should be explained here. Their graphical representation can be complementary to the text.

d) Research team:

What research team is responsible and what their role in the study will be should be clearly stated.

e) Contact details (research team/participant):

Communication throughout the study should be enabled for both research team and participant. Valid contact details should be stated in this part of the ICF.

f) Date:

The ICF should correctly document how and when the informed consent process took place, and who was involved in the process. Dates should be completed only by the data subject or the data subject's legally authorized representative or in the case of a child, the parent(s) or legal guardian(s) of the child.

g) Copy:

The data subject (or representative) should be given a copy of the consent form. It is important that a Form of Withdrawal / Study Discontinuation Form is also provided and is at all times available to the participant.

It is also crucial that the aforementioned elements are written in plain language and that they can be easily understood by the average enrolled data subject. In the case of other nationalities, all documents should be officially translated in their language before being signed. Please see the subclause on consent form wording in this guide.

9.4 Appropriate consent form wording

Consent forms, and their accompanying GDPR transparency notices, are legal documents and need to ensure compliance with data protection, ethical and legal requirements. On the other hand, in order to be informed, data subjects need to understand what they are being asked to consent to. The wording of these instruments therefore has to find a delicate balance between formality and comprehension. It is a frequent complaint raised by patient organisations that informed consent forms for clinical trials are very long and complicated. There is a similar risk for consent forms for the use of digital health innovations and for the collection of health data.

Some basic good practices include layering the information so that it can be understood in incremental levels of detail, which aids understanding, even if all of the levels of detail eventually need to be understood. Diagrams and images as a supplement to written text can be helpful at explaining concepts, even if the written text is the formalised and binding consent agreement. Lay friendly terms can often be substituted for clinical or technical jargon, and should always be preferred although sometimes it is helpful to provide both the jargon wording and the explanation together. Symbolic icons can help with understanding and with navigation.[3]

Some of the ways in which research data are handled, such as the separation of scientific data from demographic data which often occurs inside research teams, needs to be carefully explained if it is a

[3] During 2021 the Italian Data Protection Authority published a public contest for the clearest information sheets with the use of icons. At the end five winners were selected and their solutions are available and freely usable (https://www.garanteprivacy.it/temi/informativechiare#2).

safeguard amongst others being used to help protect the data. It is sometimes appropriate to commit to destroying the identifying data after a certain interval, whilst retaining the scientific data, but taking care that the distinction between these might be contextual.

It is often difficult to so robustly anonymise a rich dataset that there is no risk of pattern recognition within the scientific data, even if demographic and other identifying information have been removed. Care therefore needs to be taken in promising the data subjects that their data will be fully anonymised or de-identified, although such terms can be used if they are explained (e.g. with a glossary) and, where appropriate, some limitations are also explained. Words like impossible (to identify) might therefore be avoided. Collecting consent only for the use of anonymised data effectively precludes the use of pseudonymous data and therefore locks out the ability to link data sets longitudinally and between data sources.

NOTE The GDPR does not apply to anonymous data. However, so that the regulations cannot be applied, it should be justified that said anonymization has really been carried out. Some member states, as in the case of Spain, only require pseudonymization to carry out health research.

Within the GDPR transparency notice, the data flows (especially between organisations and countries) and the information security measures that will be adopted, are often described at a high level. This is where a diagram can be useful.

Descriptions within the consent form or the GDPR transparency notice that only cover how the information will be stored during the project imply the data are stored only during the project. Such consent will not allow the storage of any data beyond the research project, so the research portion of the data cannot be shared or reused for other research purposes. It is best to avoid promises that the data will be seen or accessed only by the research team: even if no subsequent reuse is intended the data might need to be accessed by technical staff for support reasons or by audit staff for governance reasons.

The concept of “fine print” or “small text” is not really about the size of the writing, but about the deliberate intention to provide the details in a form that the reader will not struggle with and therefore will not properly read or understand. It goes against the spirit of transparency and against the principle of informed consent.

9.5 The management of consent

9.5.1 General

The management of consent represents a central element between those who collect the patient’s choices leading to the production of the consent document, those who preserve the consent document and those who, for various reasons, access information in the document itself.

Such management should be compliant with the main international standards of the sector (ISO/TS 17975, ISO/IEC TS 27560), as well as fully compliant with the GDPR.

9.5.2 Access policy

The personal data concerning health are recognised as a special category of data in the GDPR, Art 9. An explicit consent is required before collecting and processing them.

EXAMPLE A management of consent that implements opt-in allows organizations to obtain explicit consent from the person, who has to execute an affirmative or otherwise active action to express consent.

9.5.3 Actors

The actors that can be involved in the process of collecting, preserving, and using consent are the data subject, the data controller/data processor, and the data recipients (who will themselves normally be data controllers).

— the data subject agrees to entrust to the data controller her/his personal data with respect to the policy provided;

— the data controller and the data processor, who processes the personal data on behalf of the data controller, commit to protect the personal data provided;

— the recipient receives the disclosure of the personal data of a person only if the person has been informed and has agreed to the processing of her/his personal data by the recipient.

9.5.4 Basic consent data

The minimum consent data required should enable the information present in the consent to be managed. Such information represents the consent as well as the criteria for processing data of subject. A data consent should contain at least the following data:

— who collects the consent;

— who preserves the consent;

— the data subject;

— the purpose of the processing;

— the actions allowed: collection, use and/or divulgation;

— possible restrictions (for example: only the general practitioner can access the patient's data);

— the period of validity.

9.5.5 Life cycle of a consent

The data subject's consent for processing of personal data passes through different states (see Figure 1) and each state transition is the consequence of an event triggered by an actor highlighted above (e.g., agreement, withdrawal).

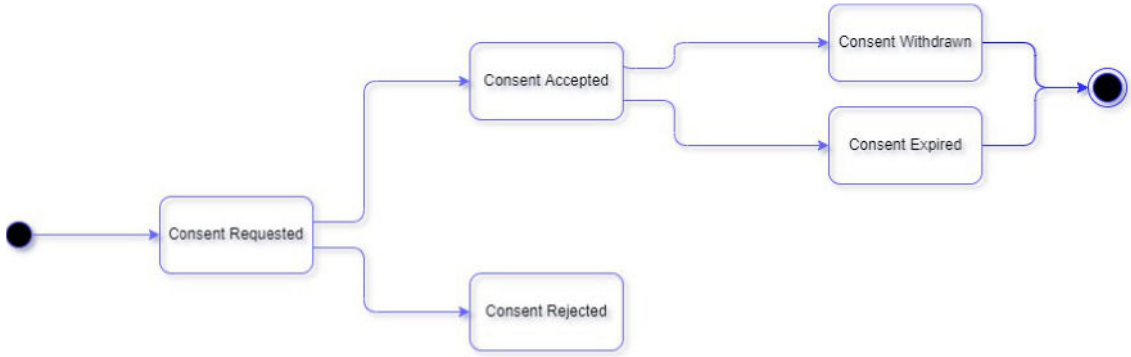

Figure 1 — Consent's life cycle

9.5.6 Use cases

The data controller should always be able to demonstrate that the data subject expressed or denied the consent for a specific purpose, that the data subject has been informed and that the procedure respects the legal bases defined in the GDPR. According to the accountability principle, the data controller should arrange pertinent technical and organisational measures to be compliant with the GDPR.

The management of consent should record the data subject's consent and the information provided when consent has been expressed. It should track every state transition. Moreover, the management of consent should regulate the access to the data subject's data respecting one's will expressed with the consent. The following use case diagram in Figure 2 describes basic functionalities required for the management of consent and the actors involved.

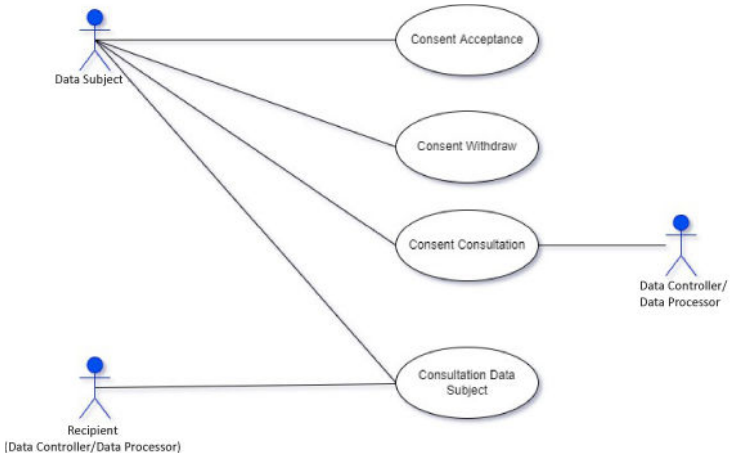

Figure 2 —Management of consent's use cases

9.5.7 Dynamic consent

Dynamic consent is an approach to informed consent that enables engagement and communication between the main actors involved in consent data management, through an interactive digital interface. It addresses the issues that are raised by the use of digital technologies in research and clinical settings. These include how to obtain informed consent in evolutionary environments (e.g., research); citizen's expectations about how their data is being used; increased legal and regulatory requirements for the management of secondary use of data, for example in biobanks.

Dynamic Consent is a practical example of how software enables researchers and clinicians to know what type of consent is attached to the use of data they hold, but also to give research participants greater understanding and control over how their data is used. It also supports the provision of a new consent if the use of the data changes, providing major transparency and enabling consent processes to reach compliance with regulatory requirements.

Bibliography

ISO 7498-2:1989, *Information processing systems - Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

ISO 13940:2015, *Health informatics — System of concepts to support continuity of care*

ISO 14155, *Clinical investigation of medical devices for human subjects — Good clinical practice*

ISO 18308:2011, *Health informatics — Requirements for an electronic health record architecture*

ISO 25237:2017, *Health informatics — Pseudonymization*

ISO/IEC 27701:2019, *Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines*

ISO/IEC/TR 26927:2011, *Information technology — Telecommunications and information exchange between systems — Corporate telecommunication networks - Mobility for enterprise communications*

ISO/IEC/TS 27560, *Information technologies — Consent record information structure*

ISO/TS 14265:2011, *Health Informatics — Classification of purposes for processing personal health information*

ISO/TS 17975, *Health informatics — Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information*

Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (ETS No. 164).

Estonian Human Genes Research Act, 2000. Available at: https://www.riigiteataja.ee/en/eli/531102013003/consolide

European Commission. Art 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation. 2 April 2013, 28.

European Commission. Art 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Art 7 of Directive 95/46/EC. 9 April 2014, 15.

Human Tissue Act, UK Parliament 2004. Available at: hta.gov.uk/guidance-professionals/hta-legislation/human-tissue-act-2004

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 (GDPR)]. Available from https://gdpr.eu/tag/gdpr/

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No

1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868

Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC. Available at https://health.ec.europa.eu/system/files/2016-11/reg_2014_536_en_0.pdf

BUDIN-LJØSNE, I., TEARE, H. J. A., KAYE, J., et al. Dynamic Consent: a potential solution to some of the challenges of modern biomedical research. BMC Med. Ethics. 2017, 18 (4). DOI:10.1186/s12910-016-0162-9

DEC. Opinion of the Data Ethics Commission - Executive Summary, 2019. Available at: https://www.bmj.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN.html

EDPB. Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research. Available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf

EDPB. Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak. Available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf

EDPB. Guidelines 05/2020 on consent under Regulation 2016/679. Available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

EDPB. Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Available at: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_en

EDPB. Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR). Available at: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-32019-concerning-questions-and-answers_en

EDPS. A Preliminary Opinion on data protection and scientific research, 2020. Available at: https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf

FDA. Information sheet on informed consent. Available at: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/informed-consent

FDA. Informed Consent for Clinical Trials. Available at: https://www.fda.gov/patients/clinical-trials-what-patients-need-know/informed-consent-clinical-trials

GEFENAS. E., LEKSTUTIENE, J., LUKASEVICIENE, V., HARTLEV, M., MOURBY, M. & Ó CATHAOIR, K. Controversies between regulations of research ethics and protection of personal data: informed consent at a cross road. Med. Health Care Philos. 2021, 25 (1) pp. 23–30

GELINAS. L., WERTHEIMER, A., & MILLER, F. G. When and Why Is Research without Consent Permissible? Hastings Cent. Rep. 2016, 46 (2) pp. 35–43. DOI:10.1002/hast.548

HALLINAN D. FRIEDEWALD M. Open consent, biobanking and data protection law: can open consent be 'informed' under the forthcoming data protection regulation? Life Sci. Soc. Policy. 2015, 11 (1). DOI:10.1186/s40504-014-0020-9

HALLINAN. D., GELLERT, R., The Concept of 'Information': An Invisible Problem in the GDPR. Scripted. 2020, 17 (2) p. 269. Available at: https://script-ed.org/?p=3885. DOI:10.2966/scrip.170220.269

https://tehdas.eu/app/uploads/2022/12/primary-recommendations-to-foster-gdpr-compliant-data-altruism-mechanisms-for-the-ehds.pdf

Human Tissue Authority annual report and accounts 2017 to 2018, 2018. Available at: https://www.gov.uk/government/publications/human-tissue-authority-annual-report-and-accounts-2017-to-2018

International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use, Guideline for Good Clinical Practice. Available at: https://ichgcp.net/

JACOB. S., DECKER, D. M., HARTSHORNE, T. S., Ethics and law for Psychologists. Wiley & Sons, New Jersey, Sixth Edition, 2011

KOSTA. E., Article 7 Conditions for consent. in Christopher Kuner and others (eds), The EU General Data Protection Regulation (GDPR): A Commentary. Available at: https://doi.org/10.1093/oso/9780198826491.003.0036

McGUIRE. A. L., BESKOW, L. M., Informed Consent in Genomics and Genetic Research. Annu. Rev. Genomics Hum. Genet. 2010, 11 pp. 361–381 [Available at: https://doi.org/10.1146/annurev-genom-082509-141711]

PORMEISTER K. Genetic research and applicable law: the intra-EU conflict of laws as a regulatory challenge to cross-border genetic research. J. Law Biosci. 2018, 5 (3) pp. 706–723. DOI:10.1093/jlb/lsy023

ROCHER. L., HENDRICKX, J. M., de MONTJOYE, Y.-A., Estimating the success of re-identifications in incomplete datasets using generative models. Nat. Commun. 2019, 10 (1) p. 3069 [Available at: https://doi.org/10.1038/s41467-019-10933-3]

ROGERS. A.C. Vulnerability, health and health care. J. Adv. Nurs. 1997, 26 pp. 65–72. DOI:10.1046/j.1365-2648.1997.1997026065.x

UTRECHT UNIVERSITY. Informed consent for data sharing. Available at: https://www.uu.nl/en/research/research-data-management/guides/informed-consent-for-data-sharing

van DELDEN. J. J. M., van der GRAAF, R. Revised CIOMS International Ethical Guidelines for Health-Related Research Involving Humans. JAMA. 2017, 317 (2) pp. 135–136 [Available at: https://doi.org/10.1001/jama.2016.18977]

WMA Declaration Of Helsinki – Ethical Principles For Medical Research Involving Human Subjects. 2008. Available at: https://www.wma.net/wp-content/uploads/2018/07/DoH-Oct2008.pdf

Writing a GDPR-compliant privacy notice (template included). Available at: https://gdpr.eu/privacy-notice