PD ISO/TS 17975:2015

BSI Standards Publication

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

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of ISO/TS 17975:2015.

The UK participation in its preparation was entrusted to Technical Committee IST/35, Health informatics.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2015

ISBN 978 0 580 79720 0
ICS 35.240.80

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 October 2015.

Amendments/corrigenda issued since publication

Date	Text affected

PD ISO/TS 17975:2015

TECHNICAL SPECIFICATION

ISO/TS 17975

First edition
2015-09-15

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

Informatique de santé — Principes et exigences des données pour le consentement dans la collecte, l'utilisation ou la divulgation d'informations de santé personnelles

Reference number
ISO/TS 17975:2015(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 215, *Health informatics*.

Introduction

This Technical Specification (TS) defines several frameworks for Informational Consent in healthcare (i.e. Consent to Collect, Use or Disclose personal health information). These are frequently used by organizations who wish to obtain agreement from individuals[1)] in order to process their personal health information. Requirements arising from good practices are specified for each framework. Adherence to these requirements will ensure the individual, as well as the parties who process personal health information, that consent to do so has been properly obtained and correctly specified. This Technical Specification covers situations involving Informational Consent in routine healthcare service delivery. There may be situations involving new and possibly difficult circumstances which are not covered in detail, but even in these situations the principles herein can still form the basis for potential resolution.

As described in 5.6, none of the frameworks described are legally mandated, and it is important to note that a jurisdiction's laws might align with one, some or even none of the frameworks described. While this Technical Specification seeks to describe what are commonly accepted as the requirements for a given framework, a jurisdiction's legal requirements may supersede the requirements described herein, and so might not permit the requirements as described to be applied absolutely.

In order to align with internationally accepted privacy principles, this Technical Specification is based on two international agreements. The first is the set of privacy principles specified by the Organization for Economic Co-operation and Development and known as the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. These principles form the basis for legislation in many jurisdictions, and for policies addressing privacy and data protection. International policy convergence around these privacy principles has continued since they were first devised. The principles require the consent of the individual for data processing activities.

The second international agreement used is the *Declaration of Helsinki*, which is used to define essential characteristics of best practices in Informational Consent management. The Declaration is a set of ethical principles regarding human experimentation. It was developed for the medical community by the World Medical Association (WMA) and is widely regarded as a cornerstone document of human research ethics. While this agreement applies directly to research on human subjects, it is intimately related to data processing, and can therefore be readily applied to the detailed requirements for Informational Consent management. It is important to note that in the context of the *Declaration of Helsinki*, the characteristics of Informational Consent were defined and developed over a number of revisions in order to remain relevant to contemporary society.

This Technical Specification specifies that a record be retained of the set of agreements and constraints granted via an Informational Consent process, and that the results of that process be made available to other parties to whom the corresponding personal health information is subsequently disclosed (see 5.10). It also defines a list of essential characteristics that the Informational Consent record should possess. These characteristics can be represented within information handling policies and used as part of an automated negotiation between healthcare information systems to regulate processing and exchange of personal health information.

Interoperability standards and their progressive adoption by e-health programmes expand the capacity for information systems to capture, use and exchange clinical data. For this to occur on a wide scale, the majority of decisions regarding the processing of data will need to take place computationally and automatically. This will in turn require privacy policies to be defined in ways that are themselves interoperable, so that interactions between heterogeneous systems and services are consistent from a security perspective and supportive of policy (bridging) decisions regarding the processing of personal health information.

A list of defined essential characteristics make up the record of the agreements granted via an Informational Consent process so as to be made available to those who wish to use the data, as well

1) Various terms are used to refer to the recipients of healthcare services. The terms patients, subjects of care, data subjects, persons or clients are all used, depending upon the relationship of the individual with the data collector and the circumstances or setting of the transaction. The term individual is used to represent a person who is a subject of care and a data subject.

as to other parties to whom the corresponding personal health information is subsequently disclosed. These characteristics might therefore be represented within policies used as part of an automated negotiation between healthcare information systems to regulate processing and exchange of personal health information.

Once consent agreement has been reached, allowable constraints defined, and the authority for the organization to collect and use or to disclose data has been established, security processes are needed to support maintenance of the consent documentation itself. Security protects the data that the organization has the authority to collect and to hold.

Why standardization of consent terminology and frameworks is desirable

The specific practices applied in obtaining and using Informational Consent vary among jurisdictions and among healthcare service settings because of variations in legislation, subject of care types and intended purposes of use. However, there is an increasing alignment globally on basic privacy principles and on a common understanding of the expectations of individuals in how their personal health data will be accessed, used and shared. International alignment of Informational Consent practices is of growing importance as personal health data are increasingly communicated across organizational and jurisdictional boundaries for clinical care, research and public health surveillance purposes. Agreed representations of Informational Consent frameworks help to clarify requirements for this international alignment. This Technical Specification describes the various Informational Consent frameworks and identifies the normative core principles that are common to all frameworks. This Technical Specification is not meant to challenge jurisdictional legislation or mandate the adoption of a specific framework. In fact, even where Informational Consent is required under legislation, the component requirements of that consent are not often specified. This Technical Specification seeks to fill that gap.

Even if two or more parties share a common policy model, this is not sufficient to support policy bridging (automated inter-policy negotiation), as the terms used for each characteristic within the shared policy model also need to be mutually understood between collectors and disclosers of health information. In other words, the characteristics of, and terms used in, the request-for-data policy need to have a computable correspondence with the terms and policies of the disclosing party's policy in order for an automated decision to be made regarding the sharing of data. Clear and consistent use of Informational Consent frameworks are an important component of that interoperability.

This Technical Specification is applicable regardless of frequency or scale of access, Use and Disclosure. However, it does assert that every access, Use and Disclosure be made in accordance with stated policies. It is possible that this might be affected on a per-data-request basis between discrete computational services, or on a per-user-session based on role, or on the basis of batch transfer of data pushed to a business area or activity. For example, claims processing might be permitted without consent as a direct and necessary purpose associated with healthcare service delivery. In this case, the business activity for which the data are used has a direct relationship to the original Purpose of Use, and purpose matching could be done for each batch transfer rather than for each individual record. The issue of how frequently the policy services are interrogated would be addressed in accordance with suitable policies applying to transactions or batches. In this way, a policy enforcement point need not consult a policy decision point nor determine consent for each record. The policy is, above all, an administrative decision that is part of the information governance activity: the policy engine automates the decision within a business activity or business area wherein the data's Purpose of Use and Informational Consent framework will have been predefined. Such pre-specified or predefined uses cannot take place in a rigorously enforced, policy-compliant manner without interoperable policy specifications, which includes the use of consistent Informational Consent frameworks.

No particular technical approach for implementing policy services or policy checking is mandated in this Technical Specification and implementers are therefore free to apply the Technical Specification to a wide range of technical approaches.

Need for formalized representation of Informational Consent decisions

Without a focused set of Informational Consent requirements which automatically apply to every data Collection, the healthcare organization cannot assume that subjects of care agree that data collected for care may be used for other purposes (e.g. research).

This classification of Informational Consent frameworks can be used in conjunction with functional roles and data sensitivity classification to support interoperability, automated decision-making related to privilege management and cross-border data flows. For example, an organization might apply a framework which combines *implied Informed Consent* for routine healthcare service delivery and support purposes with one which requires more explicit (but also informed) consent for follow on purposes of Use. By undertaking this alignment, the organization ensures that purposes to which data are put, and for which data are disclosed, are done in a way with which the subject of care agrees, and which meets ethical and legal requirements.

Inter-relationship with other standards

This Technical Specification can be used as a semantic complement to ISO/TS 22600 and ISO/TS 13606-4, both of which provide formal architectural and modelled representations of policies but do not themselves include requirements for consent. However, it is not a requirement to adopt either of these two Technical Specifications in order to use this classification of Informational Consent frameworks.

ISO/TS 22600-2 defines a generic architectural approach for policy services and a generic framework for defining policies in a formal way. However, like any generic architecture, a structural framework to support policy interoperability has to be instantiated for use. A policy domain also needs to specify which Informational Consent characteristics must be taken into account when making processing decisions. The policy domain needs to specify a high-level-policy model containing those characteristics to which all instances of that kind of policy conform.

There are other standards that define interoperability vocabularies which might also be used to instantiate parts of a policy. ISO/TS 21298 defines a vocabulary for functional and structural roles. ISO/TS 13606-4 defines a standard vocabulary for the sensitivity of EHR data (and replicates the ISO/TS 21298 vocabulary for functional roles). ISO 10181-3 provides the definition of access control information (ACI) essential to defining access control policy.

ISO/TS 14441:2013 defines privacy requirements for EHR systems. It includes several requirements for recording Informational Consent, as well as minimum data to be recorded, and provisions for emergency access.

ISO/TS 14265:2011 defines the range of purposes for which personal health data might be used in healthcare service delivery, and describes the purposes of use for which Informational Consent might be required.

ISO/TS 13606-4:2009 defines a policy model for requesting and providing EHR extracts (i.e. for one particular case to which this Technical Specification might be applied). ISO/EN 13606-4 also defines a standard vocabulary for the sensitivity of EHR data.

ISO 22857:2011 describes the transmission of data across national/jurisdictional borders or the situations where data are deliberately made accessible to countries/jurisdictions other than where they are collected or stored. One key requirement of the standard is that this processing is carried out in a fashion that is consistent with the purposes and consent obtained during the original data Collection and, in particular, all disclosures of personal health data be made only to appropriate individuals or organizations within the boundaries of these purposes and Informational Consents.

ISO 27799:2008 describes information security best practices for healthcare. It includes Informational Consent requirements for policy implementation, electronic messaging, access privilege assignment, and data protection and privacy.

ISO/TS 21298:2008 defines a vocabulary for functional and structural roles. These will support the instantiation of Informational Consent policies.

The proposed description of Informational Consent frameworks will provide a semantic contribution to the effective use of these other ISO Technical Specifications. It might also be relevant to other security-related ISO standards and specifications.

European Community Directive 95/46/EC "On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data" OJ L281/31 - 50, 24 October 1995.

The authors of this Technical Specification have given special consideration to existing and planned work in HL7 and elsewhere that supports interoperability of consent-related data structures.

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

1 Scope

This Technical Specification defines the set of frameworks of consent for the Collection, Use and/or Disclosure of personal information by health care practitioners or organizations that are frequently used to obtain agreement to process the personal health information of subjects of care. This is in order to provide an Informational Consent framework which can be specified and used by individual policy domains (e.g. healthcare organizations, regional health authorities, jurisdictions, countries) as an aid to the consistent management of information in the delivery of health care services and the communication of electronic health records across organizational and jurisdictional boundaries.

The scope of application of this Technical Specification is limited to Personal Health Information (PHI) as defined in ISO 27799, "*information about an identifiable person that relates to the physical or mental health of the individual, or to provision of health services to the individual. This information might include:*

— *information about the registration of the individual for the provision of health services;*

— *information about payments or eligibility for health care in respect to the individual;*

— *a number, symbol or particular code assigned to an individual to uniquely identify the individual for health purposes;*

— *any information about the individual that is collected in the course of the provision of health services to the individual;*

— *information derived from the testing or examination of a body part or bodily substance;*

— *identification of a person, e.g. a health professional, as a provider of healthcare to the individual.*"

Good practice requirements are specified for each framework of Informational Consent. Adherence to these requirements is intended to ensure any subject of care and any parties that process personal health information that their agreement to do so has been properly obtained and correctly specified.

The Technical Specification is intended to be used to inform:

— discussion of national or jurisdictional Informational Consent policies;

— ways in which individuals and the public are informed about how personal health information is processed within organizations providing health services and health systems;

— how to judge the adequacy of the information provided when seeking Informational Consent;

— design of both paper and electronic Informational Consent declaration forms;

— design of those portions of electronic privacy policy services and security services that regulate access to personal health data;

— working practices of organizations and personnel who obtain or comply with consent for processing personal health information.

The Technical Specification does not:

— address the granting of consent to the delivery of healthcare-related treatment and care. Consent to the delivery of care or treatment has its own specific requirements, and is distinct from

Informational Consent. **Note** that as Consent to Treatment and Care are outside the scope of this Technical Specification, the phrase "informational consent" is hereafter supplanted by the shorter "consent". In every case, it is Informational Consent that is intended;

— specify any jurisdiction's legal requirements or regulations relating to consent. The focus is on frameworks, not on jurisdictional legislation or its adequacy in any given jurisdiction. While care has been taken to design the frameworks so that they do not conflict with the legislation in most jurisdictions, they might challenge some existing practices. This Technical Specification uses an approach that allows organizations or jurisdictions to select a subset of those frameworks which best fit their law culture and approach to data sharing;

— specify what consent framework is to be applied to a data classification or data purpose as this may vary according to law or policy, although some examples of implementation profiles are provided in an informative Annex;

— determine the legal adequacy of the information upon which the consent is based or possible legal consequences of inadequate information;

— specify the data format used when consent status is communicated. The focus is on the information characteristics of consent, and not the technology or medium in which the characteristics are instantiated;

— specify how individuals giving Informed Consent come to be informed of the responsibilities, obligations and consequences related to granting consent;

— specify how individuals are to be informed of the specifics of the data, data sharing or data processing concerned;

— specify how consent itself or the specific activities of the consent process are to be recorded; only that they be recorded. Specific requirements on recording consent in EHR systems are given in ISO/TS 14441, 5.3.2;

— specify any information security requirements (e.g. the use of encryption or specific forms of user authentication) as these are the subject of other standards (e.g. ISO 27799).

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply. Capital letters are used to indicate that these terms are kinds of proper noun and have a specific meaning in privacy regulation. This specific use of the terms is indicated by initial capitalization within the text.

3.1
anonymization
process that removes the association between the identifying data set and the data subject

[SOURCE: ISO/TS 25237:2008, 3.2]

3.2
Assumed Consent
Informational Consent (3.20) done in the absence of any formal recorded or verbal indication of agreement or any overt action (or inaction) on the part of the data subject

Note 1 to entry: Assumed Consent is most often done by care providers and information collectors.

3.3
Authorization
granting of privileges which includes the granting of privileges to access data and functions

[SOURCE: SKMT derived from ISO 7498-2, the granting of rights, which includes the granting of access based on access rights]

3.4
Collection
<of data> to obtain data by any means including that of viewing it

[SOURCE: ISO/TS 14265:2011, term derived from "Collected".]

3.5
consent
agreement, approval or permission as to some act given voluntarily by a competent person

[SOURCE: Black's Law Dictionary, 2008]

3.6
data subject
identified or identifiable natural person that is the subject of personal data

Note 1 to entry: With the *Collection* (3.4) of their data, a *subject of care* (3.32) automatically becomes a data subject.

[SOURCE: ISO/TS 14265:2011, 2.10]

3.7
Denial
refusal of *Informational Consent* (3.20)

Note 1 to entry: Denial is sometimes called *Dissent* (3.9). Denial can apply to the *Collection* (3.4), *Use* (3.33) and/or *Disclosure* (3.8) of data for all or some specific data and/or Purpose(s) of Use as specified by the *subject of care* (3.32).

3.8
Disclosure
<of health information> divulging of or provision of access to data

[SOURCE: ISO/TS 25237:2008, 3.20]

Note 1 to entry: Whether the recipient actually looks at the data, takes them into knowledge or retains them is irrelevant to whether Disclosure has occurred. Disclosure occurs inside the organization if the data are made available to someone who is not authorized to have it, or it is used for a purpose not authorized. Disclosure is justified if authorized. Disclosure is not justified if not authorized.

3.9
Dissent
refusal of *Informational Consent* (3.20)

Note 1 to entry: Dissent is sometimes used as an alternative term for *Denial* (3.7).

3.10
Expressed Consent
Informational Consent (3.20) that is freely and directly given, expressed either viva voce or in writing

Note 1 to entry: Can also refer to the details of the process of obtaining Informational Consent.

3.11
Expressed Denial
refusal of *Informational Consent* (3.20) that is freely and directly given, expressed either viva voce or in writing

Note 1 to entry: Can also refer to the details of the process of *Denial* (3.7).

3.12
healthcare organization
organization involved in the direct or indirect provision of *healthcare services* (3.14)

Note 1 to entry: Service could be to an *individual* (3.19), group or population.

3.13
healthcare professional
person who is entrusted with direct or indirect provision of defined services to a *subject of care* (3.32) or a population of subjects of care

[SOURCE: CEN ENV 1613:1995]

3.14
healthcare service
service provided with the intention of directly or indirectly improving the health of the person or populations to whom it is provided

[SOURCE: ISO/TS 13606-5:2010, 3.28]

3.15
identifiable person
one who can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

[SOURCE: ISO 22857:2013, 3.7]

3.16
identification
process of using claimed or observed attributes of an entity to single out the entity among other entities in a set of identities

[SOURCE: ISO/TS 25237:2008, 3.24]

3.17
identity
Collection (3.4) of data items, such as official name, postal address, etc. that are required for naming non-ambiguously a given person

3.18
Implied Consent
Informational Consent (3.20) that is freely and directly given, indicated by an action or an inaction rather than a formal verbal or written indication of agreement on the part of the *data subject* (3.6)

Note 1 to entry: This is derived from *Expressed Consent* (3.10).

3.19
individual
single discrete entity

Note 1 to entry: This includes a distinct person or organization.

Note 2 to entry: The term may refer to a person who is a *subject of care* (3.32), a patient, a *data subject* (3.6), a client, a consumer or any other person.

3.20
Informational Consent
consent provided for the *Collection* (3.4), *Use* (3.33), *Disclosure* (3.8), or any data processing activities of *personal information* (3.25)

Note 1 to entry: As opposed to *consent* (3.5) for treatment or care, this includes *Denial* (3.7) by the *data subject* (3.6) of certain data processing activities, or constraints and conditions that the data subject might place on those activities.

3.21
Informed Consent
Informational Consent (3.20) process that provides the *data subject* (3.6) with explanations that will help that data subject in making educated decisions about whether to begin or continue participating in data *Collection* (3.4), *Use* (3.33) or *Disclosure* (3.8) of *personal information* (3.25)

Note 1 to entry: Can also refer to the outcome of the process of Informed Consent.

Note 2 to entry: Informed Consent is an ongoing, interactive process over the lifetime of the data rather than a one-time information session.

Note 3 to entry: This was adapted from ICH "Informed Consent" by changing the phrase from *"in a trial"* to *"in data Collection, use …"*

3.22
Opt-in
process or type of policy whereby the data subject is required to take a separate action to express specific, explicit or prior *consent* (3.5) for a specific type of processing

3.23
Opt-out
process or type of policy whereby the *data subject* (3.6) is required to take a separate action in order to withhold or withdraw *consent* (3.5) from a specific type of processing

Note 1 to entry: In the case of Opt-out, *Implied Consent* (3.18) exists for the collecting organization to process the *personal information* (3.25) unless the *individual* (3.19) explicitly denies or withdraws permission. Opt-out is also a process provided by a data collecting organization in order for a data subject to deny or withdraw permission to perform a specific type of processing.

3.24
personal health information
PHI
information about an *identifiable person* (3.15) that relates to the physical or mental health of the *individual* (3.19) or to provision of health services to the individual

[SOURCE: ISO 27799:2008, 3.1.9]

Note 1 to entry: Such information might include the following:

a) information about the registration of the individual for the provision of health services;

b) information about payments or eligibility for health care in respect to the individual;

c) a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes;

d) any information about the individual that is collected in the course of the provision of health services to the individual;

e) information derived from the testing or examination of a body part or bodily substance;

f) identification of a person (e.g. a health professional) as provider of healthcare to the individual.

Note 2 to entry: Personal health information does not include information that, either by itself or when combined with other information available to the holder, is anonymised, i.e. the *identity* (3.17) of the individual who is the subject of the information cannot be ascertained from the information.

3.25
personal information
information relating to an identified or identifiable natural person

[SOURCE: EU Directive 95/46/EC, MEDSEC]

Note 1 to entry: To determine whether a *data subject* (3.6) is identifiable, take account of all the means which can reasonably be used by the entity holding the data, or by any other party, to identify that individual.

3.26
privacy breach
situation where *personal information* (3.25) is collected, accessed, used or disclosed in an unlawful manner or in violation of one or more relevant privacy policies

[SOURCE: ENV 12924:1996, adapted from security breach.]

3.27
privacy control
technical and organizational measures aimed at mitigating risks that could result in *privacy breaches* (3.26)

Note 1 to entry: Privacy controls include policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management or legal in nature.

Note 2 to entry: Control is also used as a synonym for safeguard or countermeasure.

3.28
privacy policy
specification of objectives, rules, obligations and *privacy controls* (3.27) with regard to the processing of *personal information* (3.25) in a particular setting

3.29
privacy principles
set of shared values governing the privacy protection of the *personal information* (3.25) over its information management lifetime

3.30
processing of personal data
processing
operation or set of operations performed upon personal data, whether or not by automatic means

Note 1 to entry: Operations can include *Collection* (3.4), recording, organization, storage, adaptation or alteration, retrieval, consultation, *Use* (3.33), *Disclosure* (3.8) by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

3.31
pseudonymization
particular type of *anonymization* (3.1) that both removes the association with a *data subject* (3.6) and adds an association between a particular set of characteristics relating to the data subject and one or more pseudonyms

[SOURCE: ISO/TS 25237:2008, 3.39]

Note 1 to entry: Pseudonymization allows, for example, a *data subject* (3.6) to use a resource or service without disclosing his or her *identity* (3.17), while still being held accountable for that *Use* (3.33). After pseudonymization, it might still be possible to determine the data subject's identity based on the alias and/or to link the data subject's actions to one another and, as a consequence, to the *data subject* (3.6) himself.

3.32
subject of care
person or defined groups of persons receiving or registered as eligible to receive *healthcare services* (3.14) or having received healthcare services

[SOURCE: ENV 12443:1996]

3.33
Use
<of health information> act of employing data or information for a specific purpose, for which access to the data is required

Note 1 to entry: Use of data implies that the data has been collected, even if simply by viewing it.

4 Symbols and abbreviated terms

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

EHR Electronic Health Record

OECD Organization for Economic Co-operation and Development

5 Consent requirements

5.1 General

This section of this Technical Specification specifies a set of good practice activities and concepts to which the concept of consent relate. Figure 1 provides an overview of the concepts and influences in the selection of a consent model, and indicates the consent assurance process that follows. These aspects are discussed further in this section.

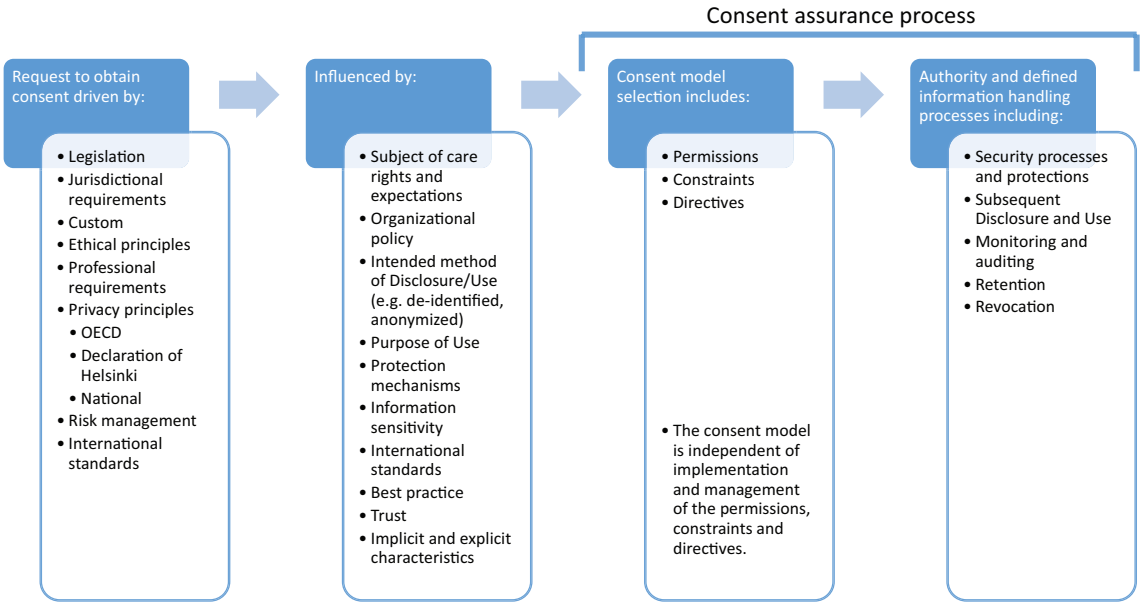

Figure 1 — Consent Concepts

Except where inappropriate, the subject of care has the right to know and so should be informed about the set of conditions associated with their granting of consent. They have a right to know what data are involved, what processes are proposed: Collection and Use and/or Disclosure, the purposes to which the data might be put, the length of time for which the data might remain active, and other specifics. Broad general descriptions of the activities intended do not adequately inform the individual.

5.2 What is Informational Consent?

Consent in the healthcare environment is widely understood as an informed and knowledgeable agreement between the data collector and the subject of care concerning certain data processing activities including its Use for various purposes including delivery of care, and includes Denial by the subject of care of certain data processing activities, or constraints and conditions that the subject of care might place on specific data or activities. It is, in effect, a contract. Informational Consent is thus a component of the privacy, security and information management policies required for the effective Use, and communication and management of information about an individual.

For ethical, and sometimes legal, reasons, information Collection, Use and/or Disclosure need to be appropriately authorized by the subject of care. Consent is a form of Authorization, provided by the individual to whom the data refers, that some information processing activity is or is not permitted. The agreement of the subject of care to the Collection, Use or Disclosure of their personal health information for specified purposes is an important step in the healthcare process.

5.3 Consent to Treatment versus Informational Consent

Consent for information Collection, Use and Disclosure is separate from Consent to Treatment. Consent to Treatment might itself be implied by attendance by the subject of care at a healthcare facility; however, since nearly all healthcare interventions lead to information being collected, it is the Use and potential onward Disclosure of this information with which this Technical Specification is primarily concerned. While subjects of care are normally content for information to be collected and used in order to provide their health care, it is still important that reasonable efforts be made to ensure that they understand how their information is to be used to support these activities and how it might be used in the future.

Informational Consent and treatment consent remain distinct from one the other, even when both are obtained as part of a single procedure.

5.4 How consent relates to privacy, duty of confidence and to Authorization

The establishment of mutual trust between a subject of care, who with the collection of his or her data becomes a data subject, and his or her healthcare providers is both a goal and a prerequisite of effective healthcare delivery. Individuals who are not informed make no meaningful decisions about how their information will be used, and thus lose an opportunity to develop appropriately trusting relationships with those to whom they give personal data.

While privacy is not an absolute right in most jurisdictions and is subject to exceptions defined by custom and legislation, a fundamental principle underlying the Use of personal health data are that it is originally collected and used for the benefit of the subject of care, and that further uses are made with the subject of care's knowledge and agreement. As part of a healthcare provider's duty of care and duty of confidence, consent forms the foundation for the Collection, Use and/or Disclosure of health information for permitted purposes by and between users, systems, organizations or policy domains which might need it. The concept of consent includes both agreement and Denial.

The act of obtaining consent from individuals reduces the risk of arbitrary Collection, Use or Disclosure of information from individuals. Loss of privacy is cumulative: with each subsequent Collection, Use or Disclosure, more of the individual's privacy is put at risk. Consent processes can inform the public of the extent of that loss. However, consent processes can also create operational inefficiency: if not well implemented, these processes will not achieve their intended objective. A consent framework which is inconsistent in design or inconsistently applied might have the effect of creating the perception of protection without actually providing it, and while increasing process and cost. Legal authority to

collect and use data or to disclose it protects those collecting, using or disclosing the data against legal risk but once legal authority is established and the data are collected, the data processing activities likewise need to be documented, and both process and data made secure. Where consent is required for Collection, Use and/or Disclosure, the process of obtaining consent provides a subject of care with general information regarding the data's protections and their rights to question, view and correct their own data and to question the organization's compliance with its information management policies.

5.5 Relationship of consent to OECD Guidelines

While consent is one of the OECD principles, those principles also state that it is only permitted to collect the information that is needed in order to deliver a defined set of services. In other words, the need to collect is predicated on the need to know. Justification of the need to know, and thus to collect, forms part of the governance and high-level policy setting of an organization or jurisdiction.

Consent is an aspect of accountability within a society, a jurisdiction and an organization or department; the consent process itself defines the organization's authority to collect data and usually describes the organization's responsibilities with respect to an individual's rights of control of their own information whatever those might be.

5.6 Relationship of consent to legislation

Privacy legislation is often based on or aligned with the OECD principles although the degree of agreement varies. As well, specific legal exceptions usually define when consent is not required. These exceptions are usually based on both ethical and practical considerations in an attempt to create balance. While this Technical Specification defines consent frameworks, it does not provide a comprehensive listing of legal circumstances under which consent is or is not required.

Legal obligations to disclose, report or communicate data can override requirements for consent, as well as requirements to match the purpose for which data was originally collected with the purposes for which the data are disclosed. In that case, the data recipient might legally be permitted to demand and to receive information without the disclosure having to fit with the original purpose(s) and without having to obtain additional consents. A jurisdiction's legal requirements will always supersede the requirements described herein since local law might not permit the described requirements to be applied absolutely. Some examples of those variations include the following:

— requirements for consent and conditions for Collection, Use or Disclosure without consent vary from jurisdiction to jurisdiction;

— exceptions to consent requirements are often defined in legislation such as law enforcement and investigations (with the authority of a court order or warrant);

— some jurisdictions require statutory authority for Collection but do not require consent; this statutory authority for Collection implies its uses but might not explicitly state them. This lack of specified purposes of Use can lead to a lack of clarity and inappropriate Use;

— some jurisdictions require a duly constituted programme as the basis for Collection but do not require consent. In this case, the programme descriptions themselves might contain the purposes description but might not;

— some jurisdictions do not require consent for Collection and Use but do require consent for Disclosure;

— retention periods for consent documents are often prescribed by regulation.

To provide sufficient meaning to the concept of consent for the Collection, Use and Disclosure of personal health information and to allow organizations to appropriately apply a fair and meaningful approach to the application of a consent process, each jurisdiction's choice of approach needs to meet a combination of ethical, legal, professional and practical requirements. This Technical Specification describes the various consent frameworks and identifies the normative core principles that are common to all consent frameworks. This Technical Specification is not meant to challenge jurisdictional legislation or mandate the adoption of a specific framework.

5.7 Expectations and rights of the individual

Consent frameworks are applied in policy and in electronic and manual processes and are driven by the following positive attributes of such processes.

a) Health information sharing supports health care.

b) Individuals expect that the necessary data will be made available for their care.

c) Individuals expect that their information will remain confidential and that only those who need access for the described purposes will have such access.

d) Organizations take account of the individual's right under law where such exists to exert control over how the information they provide is used or further disclosed;

e) Individuals expect to have knowledge of what data about them is held, how it is used and disclosed, and that it is appropriately secured.

f) Individuals expect organizations holding their personal information to be open about organizational information sharing and protection practices.

g) Controlled access to information maintains confidentiality and appropriate use of health information.

h) Purposes of Use are defined[2)].

i) The conflict between the protection of the individual's privacy and the benefits to society from the broader use of personal health information are resolved through the following:

   — evaluation of benefits versus risks of negative consequences;

   — transparency of policies related to Use, Disclosure and protection;

   — individual control over Disclosure through the use of keywords or locks;

   — use of anonymized data, in those cases where identity is not needed;

   — the minimization of Disclosure to accomplish the desired purpose.

5.8 Consent Directives

In some jurisdictions, subjects of care are permitted to express their desire by placing a Consent Directive on their data. This Directive might be authorized under policy or under law. The Directive might affect how data are used or how it may be disclosed, and might be subject to limitations or override provisions. One example is a Disclosure Directive which blocks disclosure to otherwise authorized recipients without the consent of the subject of care.

5.9 Consent is related strongly to Purpose of Use

Informational Consent is the agreement by a subject of care to permit information about them to be collected, used and/or disclosed for specified purposes. It is in order to ensure that the subject of care understands and agrees with the use of their data and by whom for whatever the specified purposes might be that consent is sought.

Typically, the Purpose of Use is such that the purpose cannot be successfully carried out without the information which is being sought from the subject of care (e.g. the purpose is *treatment and care* and the data sought is essential to providing that treatment and care). Whether purposes are stated explicitly or it is assumed that they are known to the individual, it is logical to make a direct connection between Collection and Use. The explicit declaration of intended purpose, combined with consent and defined constraints prior to granting access, helps to ensure that users understand that access does not imply that Use or Disclosure is also permitted for other undeclared or inconsistent purposes. Together, consent

2) ISO/TS 14265:2011.

requirements and Purpose of Use help bring clarity to situations where there are multiple and potentially conflicting contextually sensitive policies for access to identical information items. Consent thus aligns the policies which apply to the original data Collection and management, additional Use over time and its Disclosure to others. Knowing the consent framework and the Purpose of Use for which access to information is intended is essential in order to determine if processing activities are appropriate.

Consent only has meaning when the subject of care knows the circumstances of how the data are to be used. Therefore, where consent is obtained (either expressed or implied), the subject of care is only able to know about and either actively or passively agree if the consent process provides enough information to inform the subject of care, thus providing the subject of care with full knowledge. Only if data purposes are stated in such a manner that the individual can reasonably understand how the information will be used or disclosed can this be accomplished. While consent should be meaningful, the definition of "meaningful" should not impose requirements that are too onerous to be implemented, but rather will describe the consent frameworks which *can* be applied.

Informing the subject of care of specific purposes can create a logistical operational disadvantage if the principle is applied in too granular a fashion. For that reason, some jurisdictions have defined broad groups of purposes, for example, grouping all healthcare delivery and support purposes into a single purpose. Exceptions can be specifically defined such as is the case where the use of health information for marketing is not permitted.

Where data are intended for new or different purposes, that new purpose might require a new consent. Therefore, it might be necessary, before granting access, to compare the two purposes and the original consent obtained in order to decide if the new Use is permitted. For example, in some jurisdictions, data collected for health care cannot automatically be used for research, nor information collected for research used for care without obtaining a new consent.

It can be the case that there is a legal requirement to obtain consent for Disclosure for one type of data re-purposing and not for others. Alternatively, consent might be generally required for Disclosure except where exceptions exist in law, or where the law is silent on the matter. After accessing data intended for one purpose, that purpose and the associated consent status might need to be recorded in an audit trail. This is the case even if the access is supported by law: there ought still to be a record of the consent if it is required and the purpose that is declared and documented.

Where data are anonymized or sufficiently de-identified, the data are often not subject to consent requirements. Anonymized data are typically used for purposes which are to the benefit of the organization, jurisdiction or society as a whole, rather than to the direct benefit the subject of care. Consent might not be required because fully anonymized data does not qualify as personal information under jurisdictional law. However, given that the risk of re-identification exists if such data are linked, some jurisdictions prohibit the disclosure of de-identified individual records without consent. That said, tools to de-identify or anonymize data are improving, as are tools to assess re-identification risk.

Sometimes Purposes of Use are implicitly assumed or permitted without explicit agreement. Purposes of Use which support the delivery of care, such as eligibility and reimbursement, are often assumed. Purposes of Use which are to the good of society are often permitted without explicit agreement, e.g. public health and safety. The public interest rationale as an exception to individual privacy might be applied comprehensively, as in the case of infectious disease reporting, or might be applied on a case-to-case basis.

Data purposes can be defined and stated according to ISO/TS 14265:2011.

5.10 Consent to Collect and Use versus Consent to Disclose

Consent from an individual is required separately for Collection, Use and Disclosure of the individual's data. That said, where only that data required to fulfil the stated Purposes of Use is collected, the activities of Collection and Use are so closely related as to create a single process, i.e. consent is typically sought to both collect and use information in a single consent-related process. Use and Disclosure activities, however, are separate from one another and consent is separately required for each. While one process might be instituted to obtain consent for both Collection and Use and for Disclosure activities, it may be appropriate to ask the subject of care to grant consent to the Collection and Use

of data for one purpose or set of purposes but permit him/her to refuse consent for its Disclosure for those same or other purposes. The two activities may not always be tied together unless the service is severely compromised by doing so. A jurisdiction may have a legal requirement to obtain consent for one process (e.g. Collection and Use) but not for another (e.g. Disclosure).

5.11 Consent is applicable to specified data

For consent to be meaningful, it requires knowledge, understanding and agreement as to how the information will be used, accessed and disclosed for each piece or group of data collected. Where one piece (or "group") of information might be deemed suitable for Disclosure in a circle of care, other "groups" of information might not be so deemed and thus require Explicit Consent, i.e. a different framework. These differences are typically related to the purpose for which the information is to be used and the data's sensitivity. For example, certain pieces of information that are deemed suitable for health care delivery are not typically disclosed for support of care, such as services billing.

By default, some organizations and systems allow clinicians with a care relationship to access everything in the EHR, and then require the organization to author policies which specifically enable a wider set of stakeholders to access certain basic information, or to narrow down the access to particularly sensitive information and secrets.

For those who need data and have authority to access and use it, strictly controlled access can be applied if the potential data flow is known and controllable along the full lifetime of the data. However, for organizations to meet their practical, clinical and ethical objectives, privacy risk can be balanced against the potential for clinical risk if the information is *not* made available. Creating appropriate balance requires that thought is put into access control design, taking into consideration both legal requirements and subject of care rights and wishes, for both clinical care and adequate privacy. The consent framework chosen has a direct effect on the effectiveness and efficiency of the implemented access, as it opens up or closes down access to data.

5.12 Consent related to Disclosure

In communicating health information, the problem is one not only of determining that a user is permitted to access particular items of information, but also ensuring that the user may use or disclose them. It is therefore essential to ensure that the context within which Collection, access, Use and Disclosure is asserted is the correct one and that the agreement made covers not only Use but Disclosure. Further Disclosure of personal health information is desirable for delivery of care outside the original collecting and using organization especially within a sharable EHR and this is often supported by specific law.

Once an organization holds data, it is often assumed that Disclosure of it by the organization for the same or similar purposes is also permitted, but this is not always the case. In addition, there is a difference between legally required and legally permitted Disclosure. Police might be able to access health records as part of a criminal investigation, but such Disclosure, while permitted by law, might not be required unless appropriately documented authority is provided (e.g. a subpoena). The circumstances of the case and the applicable law will determine the appropriate action.

5.13 Exceptional access

In jurisdictions where consent policies do not permit routine access, a positive activity can be invoked in exceptional situations where a second set of permitted activities is appropriate, potentially enabling access which standard policy does not permit. Sometimes known informally as *"break the glass"* or *"consent override"* this exceptional access to otherwise unavailable data might apply to select persons or roles or to specific situations. The invocation of an exceptional access policy might occur when the subject of care is incapacitated but where, as is the case in emergency care, it is assumed that he or she would prefer the information to be made available. The invocation might also occur where an individual is a present danger to himself/herself or to others, or where public health is threatened. Such conditions are often specified in law.

A critical factor is that the additional activity is authorized by a policy that in many instances is either not written down or is not documented in a way that people think of as being a policy. The ensuing

consequence is that people think of it as overriding the policy, when in practice they are either fulfilling a documented exception which overrules a constraint in the policy, or they are invoking the *second* policy because its criteria have been met. Neither policy is actually being over-ridden, both are being fulfilled; policy is not ignored or bypassed, a situation which leads to unregulated behaviour.

The information having already been collected, this access policy applies only to uses and disclosures, and while it is often referred to as a policy override, a consent override or a Consent Directive override the term override is a misnomer. The two policies, documented and cross-referenced, establish the criteria wherein the policy which permits access is embedded in the policy which initially restricted it.

The policy which defines the exception and thus permits access might be more stringent or more permissive than the original policy which restricts such access. The application of a policy which permits an exception, which permits access, can have additional protections applied in order to ensure that such activity is not undertaken lightly: it might also be subject to additional access controls, the activity might require that the action be invoked by two authorized persons together, it might require special keywords or passwords, it might require additional notification and/or increased monitoring and auditing of the activity.

5.14 Challenges associated with obtaining consent

It is acknowledged that undertaking the consent process can be difficult, either because the subject of care's age, disabilities or circumstances have prevented them from becoming informed about the likely uses of their information, or because they cannot effectively communicate their decision. In the former case, extra care will ensure that information is provided in a suitable format or language that is accessible to the subject of care and will also ensure that it has been understood. Different jurisdictions have differing legal and process requirements to judge if and when young people are presumed to be competent for the purposes of Consent to Treatment and are therefore entitled to the same duty of confidentiality as adults. In some jurisdictions, subjects of care under the legally specified age but who are judged to have the capacity and understanding to take decisions about their own treatment are also entitled to make decisions about the Use and Disclosure of information they have provided in confidence.

Where those who perform data Collection are aware of the surrounding circumstances, there is less risk that the individual's ability to communicate their consent decisions is diminished.

6 Consent frameworks

6.1 Giving consent meaning

Consent is the set of agreements and constraints which the informed and knowledgeable subject of care agrees are permitted to apply to his or her data Collection, Use and/or Disclosure. It is one form of Authorization that something may take place.

In the context of health information and healthcare service delivery, consent is also the process whereby a set of constraints is agreed so that information may be collected and used or disclosed. However, it is also the outcome of the process.

For the consent process to be valid, consent should be

— given by the client, subject of care, data subject, their substitute decision maker or representative,

— knowledgeable,

— voluntary (not obtained through deception or coercion),

— related to the information in question, and

— applied to relevant information processing activities both by collector/user and discloser.

The following general principles, in no particular order of importance, apply.

a) Consent is applied to relevant information processing activities.

b) For consent to be valid, the subject of care is informed of the circumstances of the data and its subsequent Use and Disclosure, its general protection, retention and other specifics as described below. With adequate information, the subject of care is able to give a valid agreement knowing that to which they agree.

c) Requirements for consent and other data protection controls should increase in effective proportion with both the harm and distress that the subject of care could suffer if the data were to be released or misused. Also, data protection should increase as the degree of benefit to the subject of care lessens. This is especially true if the subject of care perceives a lack of knowledge of the data Use or where there is no direct benefit to the individual. Where benefit to the subject of care is lessened, for example when using healthcare data for research, controls should increase to protect the subject of care from harm. One of these controls is obtaining consent.

d) Consent for Collection implies consent for Use where purposes are specifically stated.

e) Only that information which is needed to deliver a programme or service and which is defined as a Purpose of Use should be collected.

f) Consent for Collection and Use are distinct from consent for Disclosure. Consent for Disclosure is tied to the Use to which it will be put by the data recipient, not the Use to which it was put by the data collector. This implies a responsibility on the part of the data discloser—the original collector—to ascertain the intended uses by the data recipient so as to ensure that the Purpose(s) of Use remains the same. That said, Disclosures[3)] might be permitted by law and limited to those where the Use is the "same" or "consistent" with the original purpose(s). Where statutory authority permits Disclosure, it often defines or implies permitted Purpose of Use, e.g. infectious disease reporting.

    1) Note on Consent for Collection and Use, as separate from Disclosure:

    2) Disclosure outside of the care organization in which information is initially collected may need Explicit Consent, but within the organization its Use may include many hundreds of staff. As well, it may be quite important for a hospital to communicate with an external care provider such as a GP. Such communication is largely assumed to be permitted for safe continuity of care and consent is not usually sought explicitly. This distinction between Use and Disclosure usually manifest in practice only when the information is sent to a more remote third party (e.g. second opinion) or, more importantly, when used for a different purpose (insurer, research, etc.). In this way, consent is strongly tied to Purpose of Use and to the need-to-know of a third party. These relationships should not be assumed, but should be actively defined.

g) An organization should not make it a condition of service that an individual grants consent to the Collection, Use or Disclosure of information beyond what is required to fulfil the explicitly specified and legitimate purposes.

h) Subjects of care should be able to give purpose-of-use-specific and separate consent where the uses of the data are not directly related to each other. For example, consent for use of information for fund raising should be available separately from consent for the use of the same information for research.

i) Where the data are required for the delivery of the service and hence the subject of care is not in a position to refuse consent, notice of data uses and routine disclosures should be made.

j) Where data Disclosure is either required or authorized by legal statute, notification of such conditions should be made.

k) Consent should not be obtained by deception or by misleading the individual.

---

3) Current discussion includes the distinction that Disclosure can mean not that data left the organization, but that it is shared internally for a purpose which is not the same as the one for which it was originally collected. The definition of what constitutes Disclosure may be different in different jurisdictions.

l) In determining the type of consent to use, the organization should take into account the sensitivity of the information, as well as the Purpose of Use. More sensitive information would require more explicit forms of consent. In fact, some jurisdictions might define all health data as sensitive thus requiring consent in all cases. Where consent is the only basis for authorizing the use of information, the organization should take into account the purpose for which the information is required (e.g. treatment or research) as this affects the type of consent, as well as the extent to which the subject of care is expected to understand the Use.

m) To whom data may or might be disclosed should be described in a manner which is understandable to the subject of care to a level of detail relevant to the environment within which the Disclosure will be made. To be valid, a consent should include a description of the group who is allowed to access and thus use the information granted in the consent. In all cases, this definition should be made at such a level that the subject of care can understand. A consent should not be asked for a larger use group than what is needed.

n) Consent can be given by an authorized representative. Representatives or substitute decision makers can be assigned through legal process or through policy for reasons of lessened capacity or other explicit reasons that apply.

o) Consent should not be used in an attempt to override obligations set out by other principles or law.

p) No reason need be given by the individual for refusal of consent. Refusal reasons should not be documented as they can imply the presence of sensitive information.

q) A subject of care's statements on Informational Consent effectively form a document which can refer to the existence of private information. Therefore, caution should be exercised when releasing the consent information, especially in the case of Disclosure refusals or where Denials exist. For example, the release of a refusal to disclose mental health or addiction data immediately informs the recipient that such data exists. Therefore, the amount of information to be disclosed should be limited to only that which is permitted to be disclosed, and should not include references to information whose disclosure is not permitted.

r) An individual should only give consent to activities related to data or information about themselves or one for whom they are an authorized representative. A person cannot give consent for the Collection, Use or Disclosure of data or information about another, for example, data about a family member or spouse that might appear in the health record of the individual. A care provider may not give consent for their subject of care unless they are their legal representative.

s) Healthcare organizations should be directed to record and manage consent and Consent Directives.

t) Healthcare organizations should be directed to adequately secure the consent process and its record in order to, if needed, provide information about the circumstances of the consent itself and the process applied and to preserve its availability, authenticity and integrity.

u) Healthcare organizations should be directed to audit access to, as well as Use and Disclosure of records in accordance with Consent Directives and policy.

6.2 Types of consent

Consent to Collect and Use or to Disclose can be specified explicitly and documented but it can also be implied or, in some cases, not required as a matter of law. Consent to use data for a particular purpose can also be implied, although it is almost always a requirement that the purposes be declared. Consent can sometimes be assumed by the data collector but where the Collection, Use or Disclosure is not agreed by the individual, either explicitly or implicitly, it is considered No Consent. This may be because consent is not required, consent is not offered or consent is not available. Any of these circumstances can result in no consent being obtained. *However, if a consent process is inadequately applied and thus*

a valid consent is not obtained, that is considered an error and is not described. The types of consent are therefore as follows.

— **Express or Expressed**: Consent to Collect, Use and Disclose personal health information is expressly given by the subject of care.

— **Implied**: Consent to Collect, Use and Disclose personal health information is implied by the actions or inactions of the individual and the circumstances under which it was implied.

— **No Consent Sought**: consent activities are not undertaken and consent cannot reasonably be implied. The most common circumstance that results in No Consent being sought is that consent is not required, and is therefore not offered nor obtained.

— **Assumed or Deemed Consent**: the collector, user or discloser activates processes based on their belief that the subject of care has, or would have, consented rather than any active or implied decision on the part of the subject of care. This is a special type of No Consent Sought.

6.3 Detailed requirements

Figure 2 describes the information that is required for express as described in 6.3.1 and implied in 6.3.2 consent. These frameworks differ in how information about the intended usage of the data and the choices an individual has about such uses are framed and how the viewpoint of the individual is obtained.

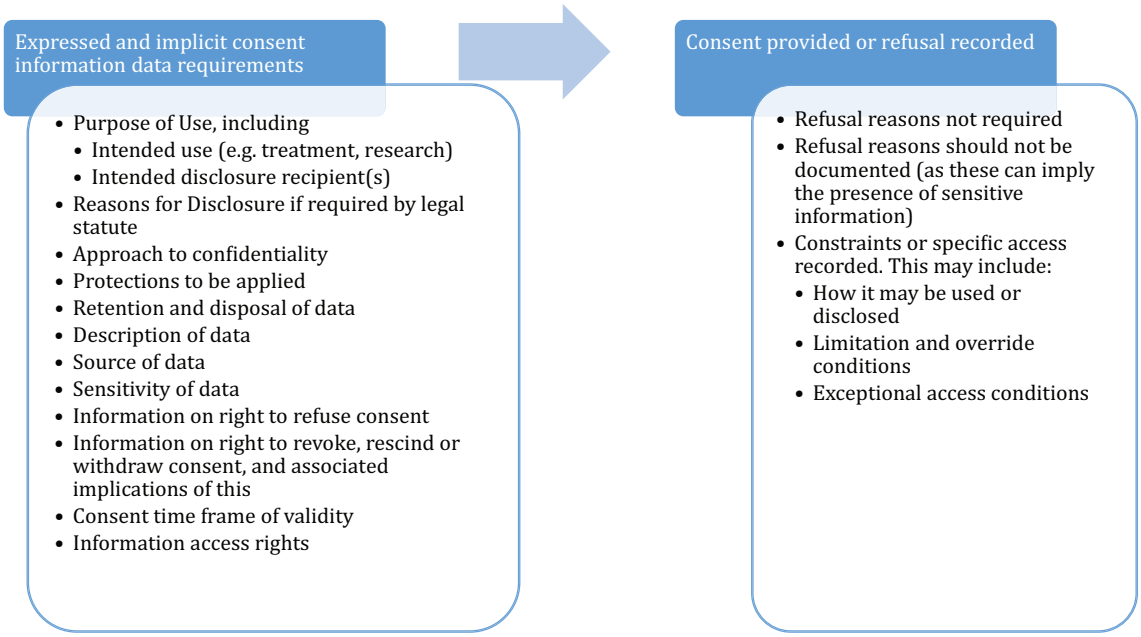

Figure 2 — Express and Implied Consent requirements

6.3.1 Express or Expressed (informed) Consent

Also known as **Explicit Consent**, this framework describes an interaction between the healthcare provider or data collector and the individual, with the active **recorded** agreement to the activity and the details of the activity by the subject of care. Express Consent should also include all of the following.

— Obtaining Consent requires a reasonable effort on the part of the data collector.

— Active Agreement can be indicated verbally or in writing.

— Agreement should be based on knowledge.

— Agreement requires that the subject of care is adequately informed. That said, it is not possible to always determine whether the subject of care is actually adequately informed. Reasonability tests should be applied to processes which might be subject to legal or ethical requirements.

— Agreement requires that for the subject of care to obtain an adequate level of knowledge about the Collection and Use and/or the Disclosure of their data, detailed information should be provided to the subject of care with respect to the data given in Figure 2.

— A description of the data which can include example data elements.

— The source(s) of the data if Collection is indirect rather than collected directly from the subject of care.

— The intended Purposes of Use including the name of the legally constituted programme or initiative which uses the data for the named Purposes of Use.

— The intended disclosures, the organizations to which the data may or might be disclosed, and the Purpose(s) of Use for which it may or might be disclosed.

— The legal or policy authority (if applicable) for the Collection and Use and/or Disclosure.

— The legal or policy authority (if applicable) which gives the data discloser the authority to disclose if Collection is indirect.

— Details about retention of the data: timeframe and intended or eventual disposition.

— The general approach to safeguarding confidentiality.

— The subject of care's rights to refuse consent and to continue to receive services in the face of refusal.

— The subject of care's right to revoke, rescind or withdraw their consent, provided reasonable notice is given. Revocation cannot be retroactive.

— The implications of either refusal or withdrawal of consent.

— The time frame for consent applicability and information regarding the refreshing of the consent.

— The subject of care's rights to have access to the information about themselves.

— Information provided should be stated in such a manner that the individual can reasonably understand. Reasonability tests should be applied where consent processes should meet legal or ethical requirements, taking into the consideration what is practical given the circumstances and setting of the data processing activity and the actors involved.

— Consent should be obtained at the time of Collection, preferably at the first contact.

— If agreement is verbal, the fact of it should be recorded.

— The individual's indication of consent and its details, including where written or that given verbally should be recorded and stored in a form that is secure, understandable, available and, in order to ensure authenticity, preserves the integrity of the record.

— The conditions of consent, and the information supplied at the time consent was obtained, should be stored securely, be available and, in order to ensure authenticity, preserve record integrity.

— A new purpose might require that a new consent be obtained, depending upon how closely the new purpose is tied to the original purpose.

— A new organization or individual to whom the data are disclosed might require that a new consent be obtained, depending upon how closely the new organization is related to one already specified.

— Exceptions might exist in law or policy; for example, if the seeking of consent would compromise the availability or accuracy of the information, or compromise a legal investigation.

— Subjects of care have a right to have knowledge of the organization's information management policy with respect to the subject of consent.

— Subjects of care should be provided with information regarding contact with the organization in case they have questions.

6.3.2 Implied (Informed) Consent

This framework describes an interaction between the healthcare provider or data collector and the subject of care, with the active agreement to the activity and the circumstances of the data Collection and Use and/or Disclosure on the part of the subject of care. To be valid, Implied Consent should include the following.

— Agreement is inferred from conduct or implied by action.

— Informed Implied Consent or "knowledgeable cooperation" includes both knowledge and action.

— "Knowledge" can be imputed based on reasonable attempts to make the public aware even if a particular member of the public does not have the knowledge but "could have or should have known".

— "Action" can include "inaction" when there is knowledge that something is occurring and steps are not taken to refuse to be involved AND if it can be shown that the person knew or had a reasonable opportunity to know that something would happen unless they objected, i.e. took action to indicate that they did not want the particular thing to happen.

— Agreement should be based on knowledge.

— Agreement requires that the subject of care is informed.

— For the subject of care to achieve an adequate level of knowledge about the Collection and Use or the Disclosure of their data, information should be provided to the subject of care or more generally to the public with respect to the data given in Figure 2:

— A description of the data which can include example data elements.

— The source(s) of the data if Collection is indirect rather than collected directly from the subject of care.

— The intended Purposes of Use including the name of the legally constituted programme or initiative which uses the data for the named Purposes of Use.

— The intended disclosures, the organizations to which the data may or might be disclosed, and the Purpose(s) of Use for which it may or might be disclosed.

— The legal or policy authority (if applicable) for the Collection and Use and/or the Disclosure.

— The legal or policy authority (if applicable) which gives the data discloser the authority to disclose if Collection is indirect.

— Retention of the data: timeframe and intended eventual disposition.

— General approach to safeguarding confidentiality.

— The subject of care's rights to refuse consent, and to continue to receive services, in the face of refusal.

— To revoke, rescind or withdraw their consent where they have that right, provided reasonable notice is given. Revocation cannot be retroactive.

— The individual should be informed of the implications of either refusal or withdrawal of consent.

— The time frame for consent applicability and information regarding the refreshing of the consent.

— The subject of care's rights and opportunities to access information about themselves.

— To have knowledge of the organization's information management policy with respect to the subject of consent.

— The relationship between the healthcare provider or data collector and the subject of care should be described. The healthcare provider or data collector should provide the following general information regarding contact with the organization in the case of questions and a privacy notice made generally available to all subjects of care and the public:

— The legal name of the entity that collects the data.

— A general description of the personal data are typically collected.

— The purposes of the Collection and processing of their personal data and the typically employed transfers of the data.

— The options and means that the subject of care may use in order to control the Use and Disclosure of their personal data.

— The means by which they can exercise their rights of access, rectification, cancellation or opposition.

— Information provided should be stated in such a manner that the individual can reasonably understand.

— The individual's consent is not generally documented, however, if documented the individual's indication of consent, the conditions of the consent and the information supplied at the time the consent was obtained should be recorded and stored in a form that is secure, understandable, available and, in order to ensure authenticity, preserves the integrity of the record.

— Consent should be implied at the time of Collection, preferably at the first contact.

— A new purpose requires that a new consent be obtained depending on legislation. It can be a matter of judgement how closely the original purpose and the new purpose align.

— A new organization or individual to whom the data are to be disclosed might require that a new consent be obtained depending upon legislation. It can be a matter of judgement how closely the original organization or organizations and the new organization are related.

— Obtaining consent requires a reasonable effort on the part of the data collector.

— Exceptions might exist in law or policy. For example, if the seeking of consent would compromise the availability or accuracy of the information and the Use is reasonably linked to the purposes of an investigation.

— There can be strong pressure from privacy commissioners to restrict the use of Implied Consent where the information to be disclosed is of a sensitive nature – as it is in health care.

6.3.3 No Consent Sought

In this framework, information may be collected and used or disclosed at will. This framework includes no consent interaction between the healthcare provider or data collector and the individual, with no agreement to the activity on the part of the individual.

— The "No Consent" state applies separately to Collection and Use and to Disclosure. These two activities can be controlled separately under law or policy.

— Authorization for collecting and using or for disclosing data might exist in law or policy without mentioning consent. In this case, consent is not required simply because no law or policy exists which requires it, or mentions it, and thus consent is not offered nor obtained.

— Authorization for collecting and using or for disclosing data might exist in law based on specifically defined circumstances as might be the case in some jurisdictions. An example is infectious disease legislation which can require Disclosure without the consent of the individual and so a consent process is not offered and consent is not obtained.

— Notice of the circumstances of the data, Purposes of Use, Disclosures, retention times and other required specifics of the process should be provided at the time of Collection or as soon as possible afterward and should anticipate possible future Disclosures and provide a general description of likely Disclosures.

Consent to Collect and Use might not be required and therefore not obtained

— if the data was collected lawfully under the provisions of Collection without consent, or

— if the information is publicly available.

Consent to Disclose might not be required and therefore not obtained

— if the Purpose of Use is the same as the original Purpose of Use for which the data was collected and that purpose is clearly in the interests of the subject of care,

— if it is used for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual,

— where authorized or required by law,

— if it is made to a barrister or solicitor who is representing the organization,

— if it is required to comply with a subpoena or warrant or order of the court,

— if it is requested for the administration, investigation or enforcing of law,

— if the information is publicly available, or

— if no law requires it. In other words, if the law is silent on the matter.

6.3.4 Assumed Consent (Deemed Consent)

In this framework, the consent of the individual is assumed by the collector or user of the information and is done in the absence of any formal recorded or verbal indication of agreement or any overt action (or inaction) on the part of the subject of care. Assumed Consent is not a true consent as the action (decision) is made by the data collector and not the subject of care. **It is a special type of No Consent Framework** and cannot be characterized as an agreement by the subject of care. In some environments, Assumed Consent is accepted as ethical and is legal.

— The assumption is made by the data collector and not by the subject of care.

— Purposes of Use for the data Collection and/or Disclosure are assumed to be known or should be known to the subject of care because they are of a ubiquitous nature within the jurisdiction and are widely known to the public. In other words, the jurisdiction provides generally and widely available information about the Collections, Purposes of Use and Disclosures.

— In using an Assumed or Deemed Consent framework, it is not possible to make assumptions about Purposes of Use that are not clearly apparent.

— Collection can be direct or indirect.

— Assumed or Deemed Consent lacks some of the characteristics associated with Explicit or Implied Consent.

— No notice or description specific to the Collection, Use and/or the Disclosure is provided at the time of Collection.

— No indication of agreement with the intended Collection, Use and/or subsequent Disclosure is made.

7 Mechanisms and process: Denial, Opt-in and Opt-out, and Override

7.1 Express or Expressed (and Informed) Denial

Denial is an outcome of Explicit Consent gathering and of making a choice rather than a pattern of choice. Denial models the concept of a secret which is unknown and the fact of the secret itself is kept secret. This negative consent or refusal of consent is called a Denial. Using a Denial a subject of care can give full access to every other piece of information and denied information is still not seen. The purpose is to prevent pressure to give a consent.[4)]

In some jurisdictions, a subject of care may be permitted to deny Disclosure as a separate action[5)] or even to deny Disclosure of specific data and/or to a specific organization or health provider or person. Explicit Denial may be permitted where data Collection is legally permitted without Explicit Consent. The difference is if information is assumed to be denied or assumed to be allowed. The desired result is to know what accesses to information are both permitted or might be granted and which ones are not permitted or might not be granted. Whether it is more expedient (and acceptable) to ask people to state what they want to happen, or what they want not to happen, is a matter of what is efficient and tractable to achieve. Asking the individual to indicate his/her preferences as a set of agreements or a set of Denials is simply the choice of assuming agreement in the face of no objection, or assuming objection in the face of no agreement. If all the information is denied by default, then a consent is needed and should be sought every time information is collected, used or disclosed. If information Collection, Use or Disclosure is allowed by default, then to have control, an individual would specifically prevent a piece of information from being collected or disclosed.

Where data are not available because the subject of care refused their consent, that refusal can sometimes be overridden in the case of an emergency: it is assumed that an incapacitated subject of care would prefer the information to be made available. Consent is often assumed for emergency care. However, in this framework denied information can't be seen even in emergency, and thus a consent or Denial should be specified separately and explicitly for emergency care as opposed to routine healthcare.

Where it exists, a Denial should be removed before Use or Disclosure can take place. A previously authored Denial will need to be revised to allow for one or more specific Disclosures (e.g. "deny access to all nurses" is changed to "deny access to all nurses except for nurses at hospital A"). Clearly, only those authorized to edit that policy stipulation can do this.

Where a Denial is permitted, this might not always be the right decision. In the healthcare setting, one might wish to indicate that other information exists, or may go as far as to include a description as to what sort of information exists but is being denied, so that it can be sought under a separate process.

Denial can be done with no constraints but be broad and generic. However, practicality and implementation issues exist related to the level of granularity of the application of Denial. There will inevitably be limits on systems such that Denial might need to apply to whole records, or subsets of records as opposed to individual data items. Decisions must be taken as to what data and under what circumstances a Denial is permitted considering: the need or wish for setting the Denial, the information being denied, and to whom, and the mechanisms for its removal. The fact that withheld information may constitute a downstream risk to the patient during future clinical encounters is part of good informing practice. The means of engaging the subject of care in the decision is as important as the end result because the desired outcome will influence the decisions as to how that engagement takes place, and how that engagement takes place will affect the eventual outcome. It may be necessary to document the individual's Denial choices and the conditions and information supplied at the time.

Where a Denial is removed, the consent process should be reapplied thus engaging the subject of care in a detailed review of consent and Denial choices. Documentation should be recorded and stored in a form that is secure, understandable and available.

---

4) Agreement to share personal health information with everybody inside a care organization but not to allow Disclosure to external organizations is both an agreement and a Denial in a single statement.

5) If Purposes of Use are described at the time of Collection, Use cannot be denied. To do so would result in an inappropriate and unnecessary Collection.

A related matter is what to do when there are conflicting policies, for example, if a subject of care permits a clinical team to see their medication list but denies them access to the psychiatric record. A conflict might arise if the psychiatric record includes medication prescriptions. Agreement and Denial stipulations have to be drafted in a way that avoids overlaps or gaps: in overlap and gap situations, the consent stipulation is indeterminate, neither permit nor deny can trump the other unless the wording clearly states this. There can be conflict of interest between a patient's wish and a professional's duty to document and share, e.g. to keep a medico-legal record of care provided and its rationale, similar to the conflicts that may arise between parental wishes regarding teenage children. A Denial to disclose also means that the information will not be available for other purposes such as health system management. For all these reasons, jurisdictions should carefully consider the design and implementation the Denial function.

7.2 Opt-in and Opt-out

Opt-in and Opt-out are patterns of choice that may be offered through a consent process.

7.2.1 Opt-in

The process of opting in affects how the consent of the individual is obtained and operates against all forms of consent that employ an active mechanism, i.e. expressed or implied. With the case of Opt-in, the individual should take the action for any consent to be valid—to actively make a choice.

7.2.2 Opt-out

The process of opting out also affects how the consent of the individual is obtained and operates against all forms of consent that employ an active mechanism, as well as those which do not, i.e. No Consent. With the case of Opt-out, the individual should take the action of indicating that they do NOT wish for their data to be included in processing. Here, too, they actively make a choice against the activity.

7.3 Override

Override is not about obtaining, documenting and complying with consent, but about when and how to operate differently against already specified consent stipulations. Some jurisdictions might permit or deny Collection, Use and/or Disclosure by the application of an additional and different policy which permits what has previously been prohibited. In practice, the organization is either fulfilling a documented exception which over-rules a constraint in a policy, or they are invoking a *second* policy because its criteria have been met. Neither policy is actually being over-ridden, both are being fulfilled; policy is not ignored nor by-passed, a situation which leads to unregulated behaviour. Where this is permitted by law or policy, an organization or person with appropriate authority and/or Authorization may do so within the constraints of the permitting policy.

For a complete set of diagrams illustrating Opt-in and Opt-out, see Annex A.

For examples of implementation profiles, see Annex B.

8 Minimum data requirements

A consent documentation record should include

— a description of **what data** are to be collected and used or disclosed,

— for **WHAT Purpose of Use**,

— to **Whom**,

— on **WHAT date the consent comes into effect**,

— **for how long** the agreement and constraints are effective,

— if/**when** the decision **has been refreshed**,

— if/**when it has been revoked**, and

— **WHAT** specific information about the data and its proposed uses, disclosures, retentions, etc. was provided to the subject of care at the time the consent was obtained,

or

— a description of **what data** are not permitted to be used or disclosed and to whom,

— for **WHAT Purpose of Use**,

— on **WHAT date**, and

— **WHAT** information was provided to the subject of care at the time.

When consent details are modified, both the original and the new consent details should be retained to provide traceability. For example, where consent for an activity or type of data was initially refused and then later obtained, it is advisable to retain both the initial refusal and the later acceptance. These records are needed for auditability.

Records of Expressed Consent should include the following general categories of data elements.

— Information about the data: Purpose of Use, activity consented to (Collection, Use or Disclosure), intended Purpose of Use, description of the data.

— Information about the actors: subject of care, data discloser (if applicable), data recipient.

— Information about the consent: date obtained, date expires, date refreshed (if applicable), date revoked (if applicable), date refused (if applicable), reference to the form or process used by the organization at the time the consent was obtained, if overrides are permitted.

A consent record should

— identify the sender, recipient and subject of care,

— include the Purpose of Use or set of purposes which are permitted to be collected and used or disclosed,

— specify the activity permitted: Collection and Use and/or Disclosure,

— include the validity date range,

— be linked directly to the data to which it applies,

— persist with the data to which it applies, and

— be secured in order to preserve confidentiality, integrity, availability in order to provide proof of authenticity of the process and the consent record.

Annex A
(informative)

Consent framework diagrams

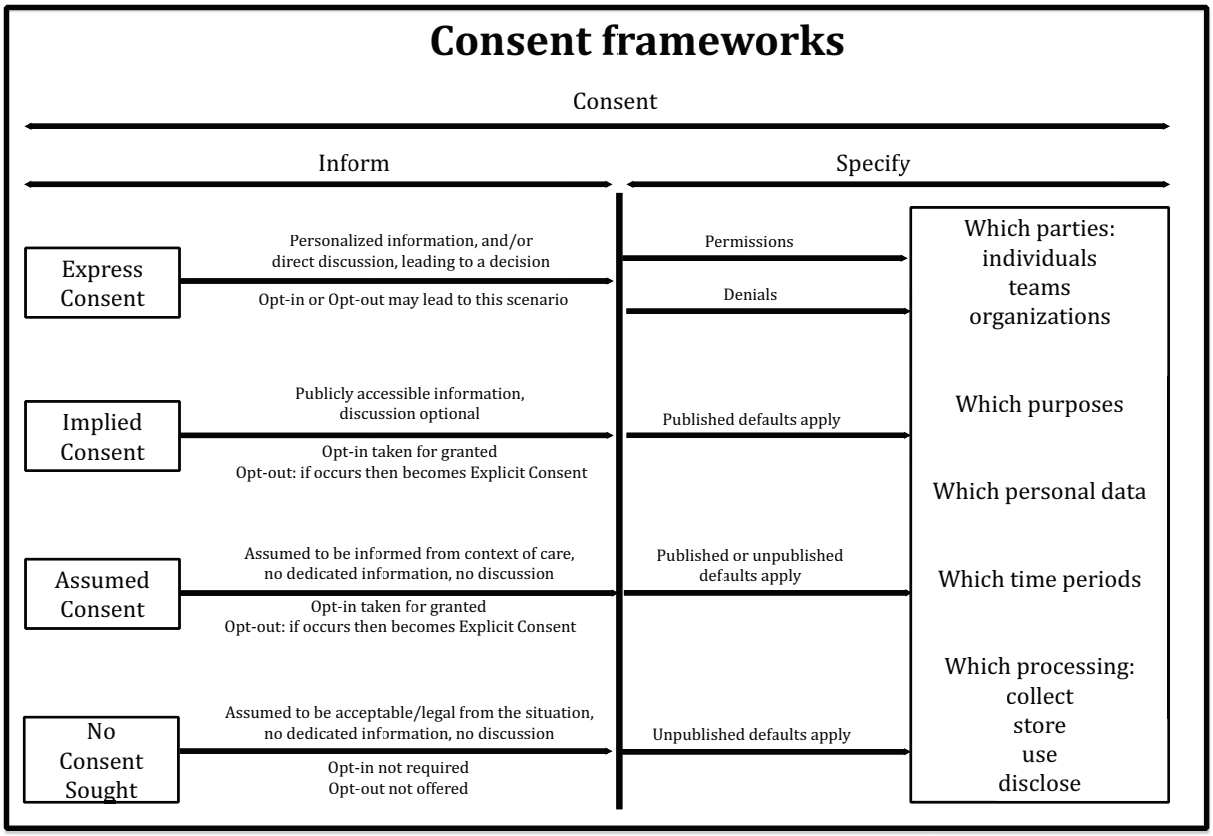

Figure A.1 — Consent frameworks

Figure A.1 describes the options that can be provided, but does not assert which options are appropriate nor seek to indicate whether not offering consent is appropriate or inappropriate. Denial can only be given explicitly, and therefore only applies in Figure A.1 to the first of the four options. In practice, agreements and Denials are two alternative (or combinable) ways of specifying what the consent agrees or disagrees to and are part of the specifying, not the informing, process. Capture and implementation of Explicit Denial specifications can arise in any of the first three options.

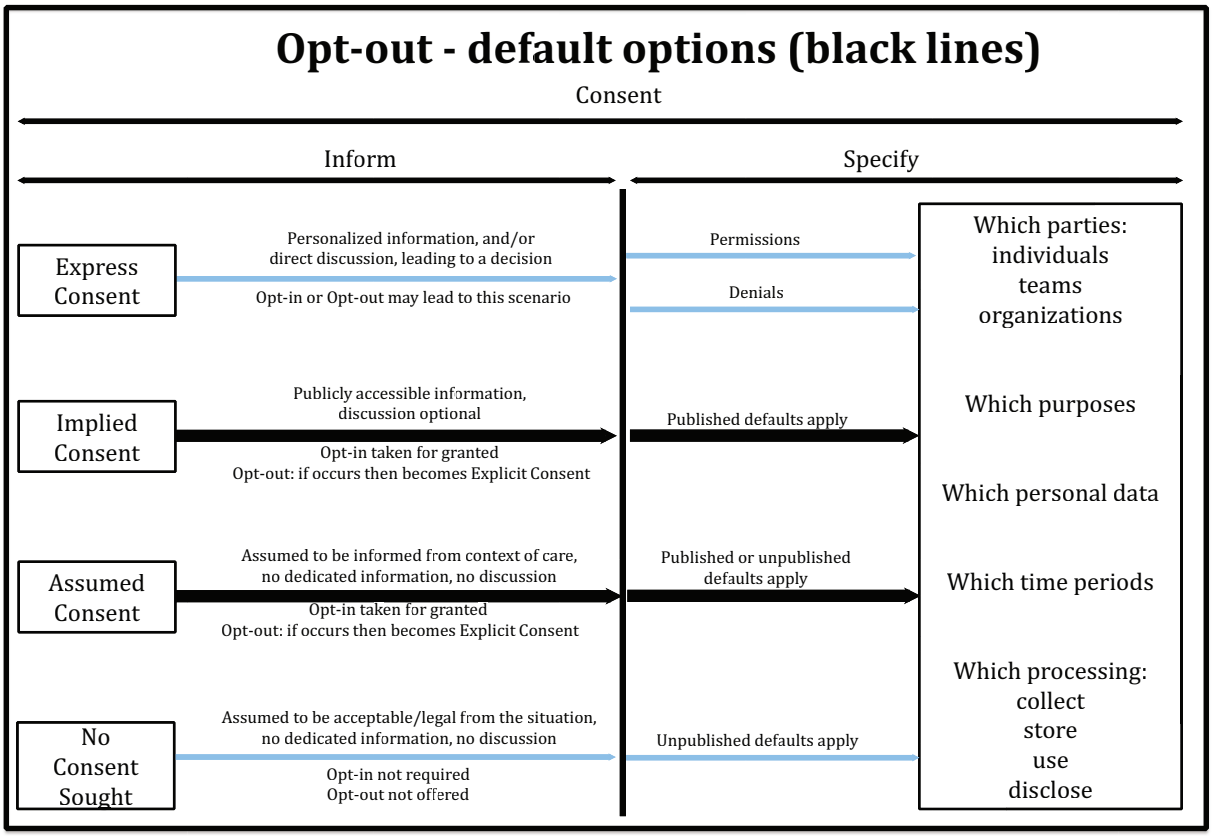

Figure A.2 — Opt-out – Default options

Opt-out constitutes a process provided by an organization collecting data whereby a separate action is required in order to withhold or withdraw consent for a specific type of processing. In this case, Implied Consent requirements exist for the organization to process personal information unless the individual explicitly denies or withdraws their agreement.

The process of opting out operates against all forms of consent that employ an active mechanism, as well as those which do not, i.e. No Consent. With the case of Opt-out, the individual should take the action of indicating that they do NOT wish for their data to be included in processing. Here they actively make a choice against the activity.

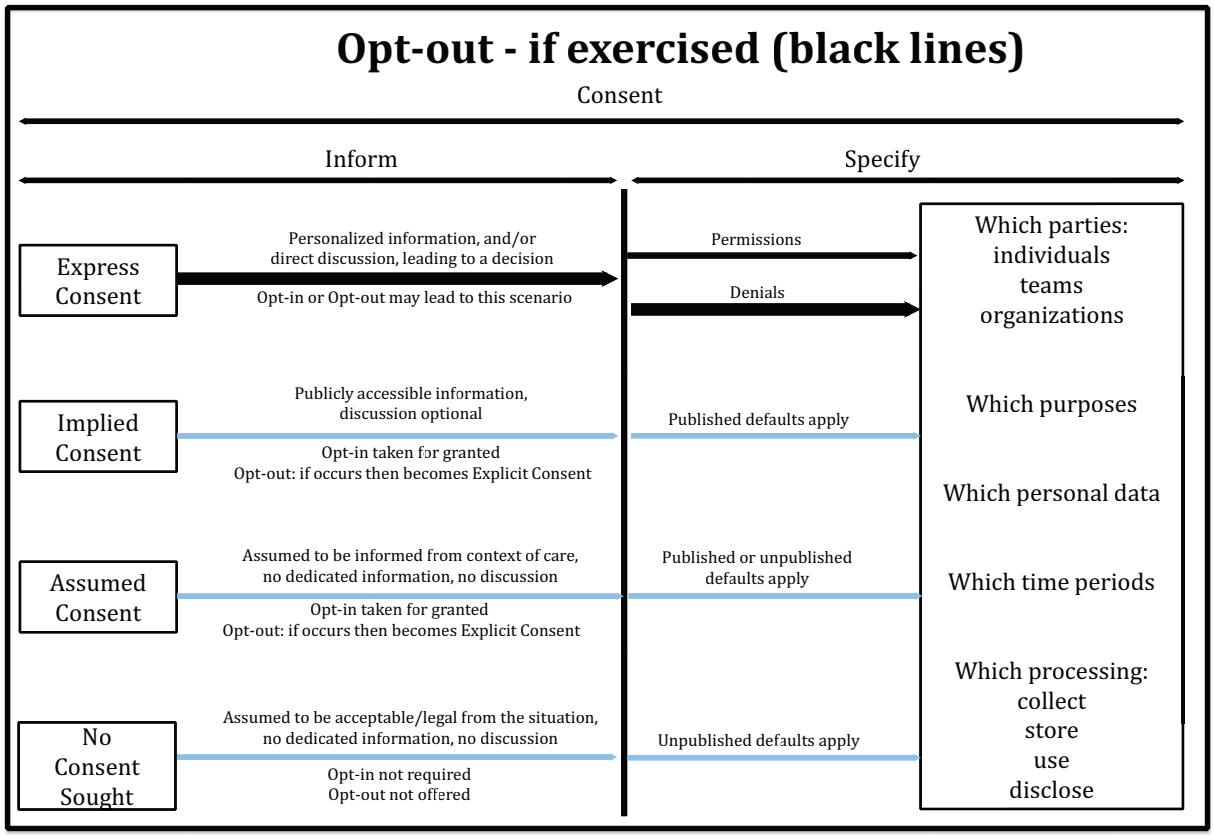

Figure A.3 — Opt-out – If exercised

Opt-out constitutes a process provided by an organization which collects data whereby a separate action is required in order to withhold or withdraw consent for a specific type of processing. In this case, if exercised, the Opt-out process constitutes a type of Explicit Consent required on the part of the organization.

The process of opting out operates against all forms of consent that employ an active mechanism, as well as those which do not, i.e. No Consent. With the case of Opt-out, the individual should take the action of indicating that they do NOT wish for their data to be included in processing. Here they actively make a choice against the activity.

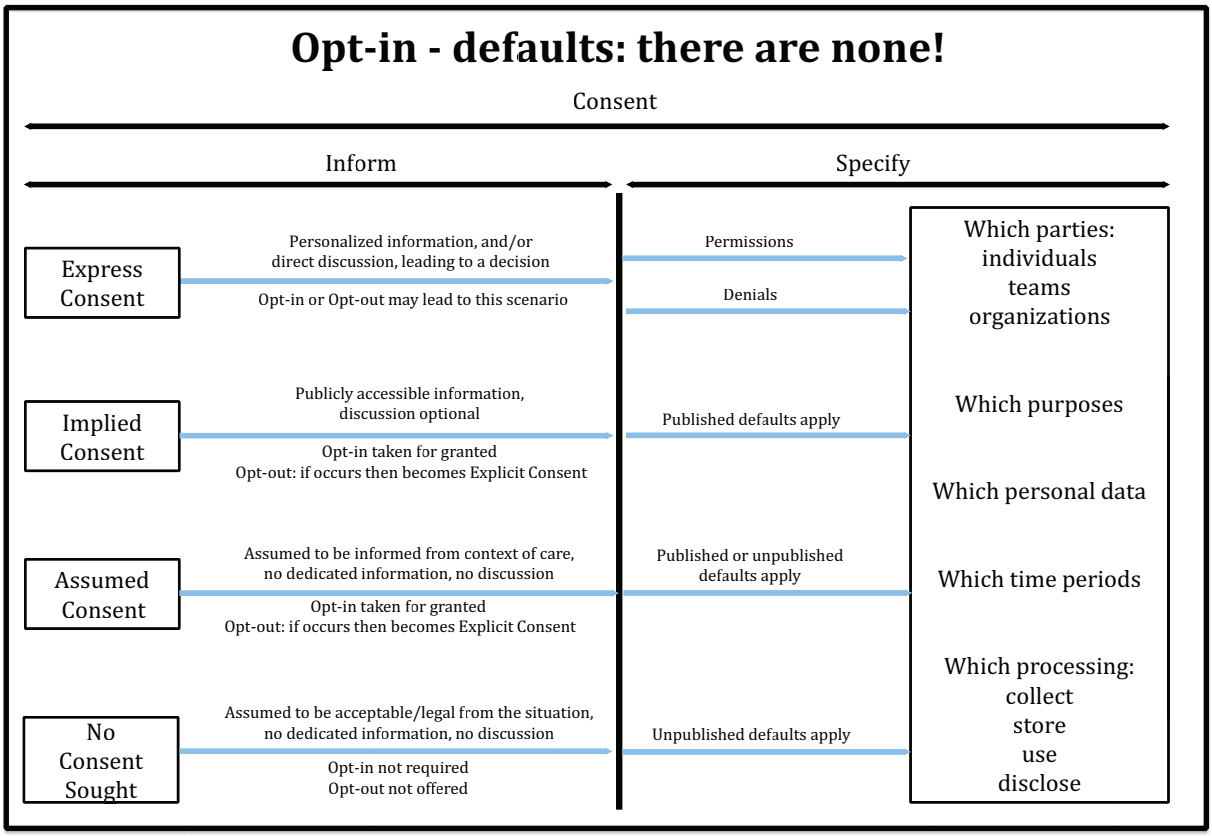

Figure A.4 — Opt-in – Defaults: None

Opt-in is a process whereby the data subject is required to take a separate action to express specific, explicit, prior consent for a specific type of processing. Personal information (and an associated Opt-in) could be collected by an external processor acting on behalf of the collecting organization.

The process of opting in operates against all forms of consent that employ an active mechanism, i.e. expressed or implied. With the case of Opt-in, the individual should take the action for any consent to be valid.

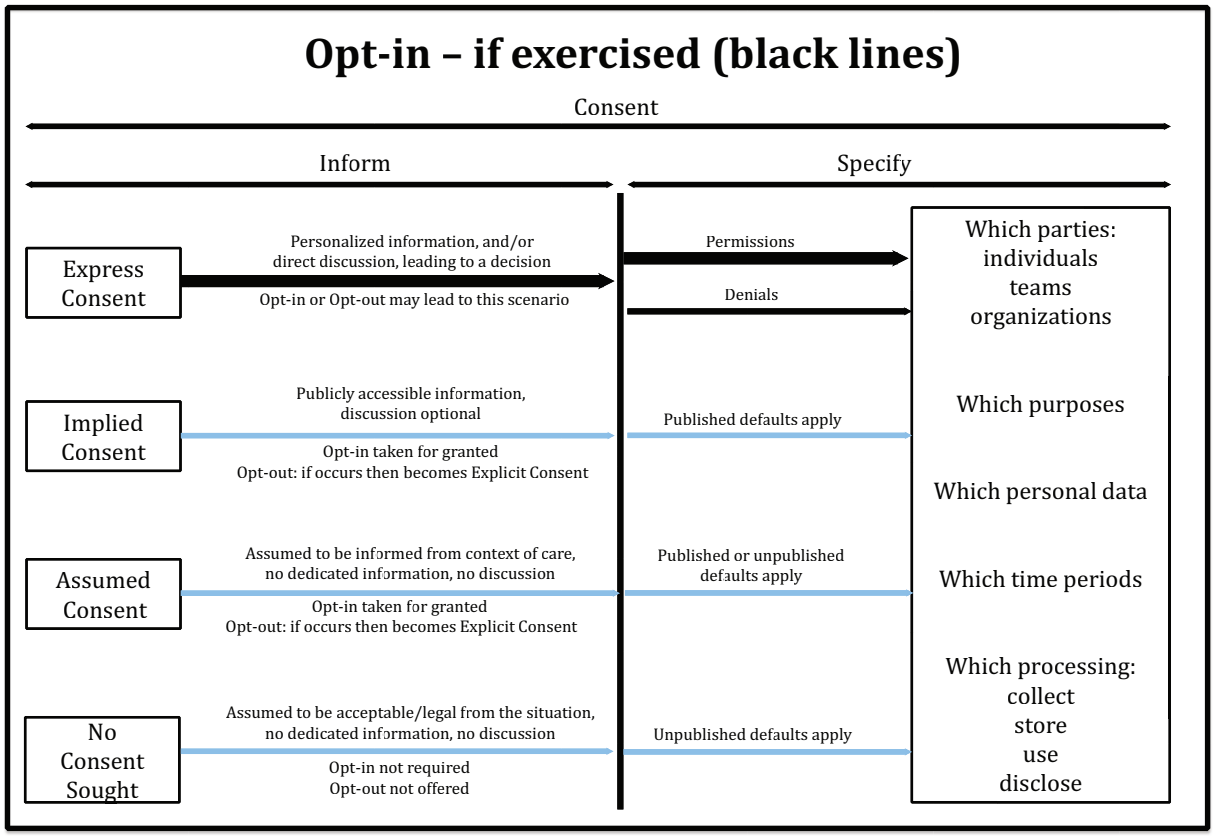

Figure A.5 — Opt-in – If exercised

Opt-in is a process whereby the data subject is required to take a separate action to express specific, explicit, prior consent for a specific type of processing. Where exercised, Opt-in is a type of Explicit Consent.

The process of opting in operates against all forms of consent that employ an active mechanism, i.e. expressed or implied. With the case of Opt-in, the individual should take the action for any consent to be valid.

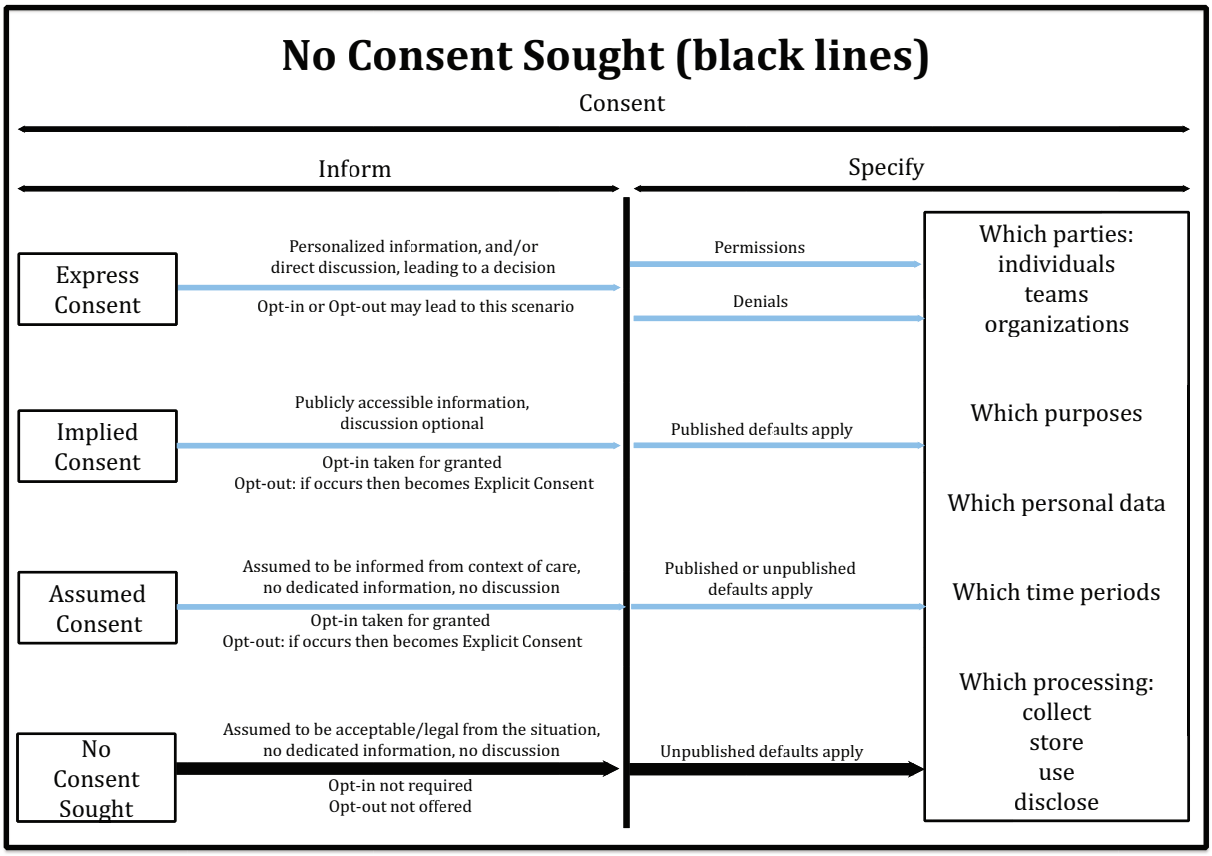

Figure A.6 — No Consent Sought

In this case, consent is not considered. No process to obtain consent is applied. Consent is not sought. There can be different reasons for this, but most of often, it is because it is not required, or is required generally but an exception exists.

The process of opting out operates against those forms of consent that do not employ an active mechanism, i.e. No Consent. With the case of Opt-out, the individual should take the action of indicating that they do NOT wish for their data to be included in processing. Here they actively make a choice against the activity.

Annex B
(informative)

Jurisdictional implementation examples

Hypothetical applications of the consent model based for implementing a "care.data" type system in England as of March 2014[6)]

In England, there is a proposal to create a comprehensive patient level healthcare database for indirect care use purposes from primary and secondary care records. A database will be created from doctor–patient interaction data and prescriptions extracted from general practice systems in coded form together with the patient's NHS Number and a limited set of other data items that potentially could identify the patient. The resulting records will go to the Health and Social Care Information Centre (HSCIC) and be linked at patient level via the NHS Number with current and historic secondary care activity data derived from hospital systems. Records for individual patients will be held within a system entitled "care.data" in pseudonymized form with identifier data being held separately from clinical data.

The aim is to form a comprehensive person level database of primary and secondary care activity for a range of healthcare purposes, including research, with, for example, data being made available in pseudonymized form to researchers.

"Care.data" can proceed in theory on the basis of the powers given to the HSCIC in the 2012 Health and Social Care Act for obtaining identifiable data "under direction from specific bodies," together with meeting fair processing requirements for the de-identified data by privacy notices being sent to all households in England.

Applying the consent model – For the purposes of providing a complex test and illustration of the consent model, the following assumptions have been made.

— Relevant "directions" will enable the HSCIC to gather patient level activity data from practices.

— If patients do not object to the use of their data, records containing the NHS Number, age, postcode sector (i.e. four characters as opposed to six characters in a full postcode) together with relevant clinical and administrative data will be sent to the HSCIC for inclusion in "care.data".

— Patients can object to the transfer of data concerned with their identity (this Opt-out of the transfer of identifiers is based on a NHS Constitution commitment and is not a legal right).

— Patients cannot object to the transfer of clinical and administrative data that does not identify them; an anonymized record will be sent from the practice when individuals object to the disclosure of their identifiers.

The courses of action that follow from the above assumptions, together with the application of the Consent Model, are set out below. The specific application of the model is shown in diagrams with black arrows, with other options greyed out.

---

6) Please note at the time of writing the rules around "care.data" and management of objections in the implementation of "care.data" were still being formulated. The basis for the "care.data" and the interpretation for objections used in this annex have been created by the author and are purely for testing and illustrating the consent model.

Scenario 1 – the patient takes no action upon receipt of a "care.data" leaflet delivered to the patient's home and it is assumed that the patient is willing for their full record (i.e. identifiable and clinical data) to flow.

Consent model application – Opt-out is not exercised, thus Implicit Consent applies in the UK (note that in other jurisdictions Assumed Consent could apply).

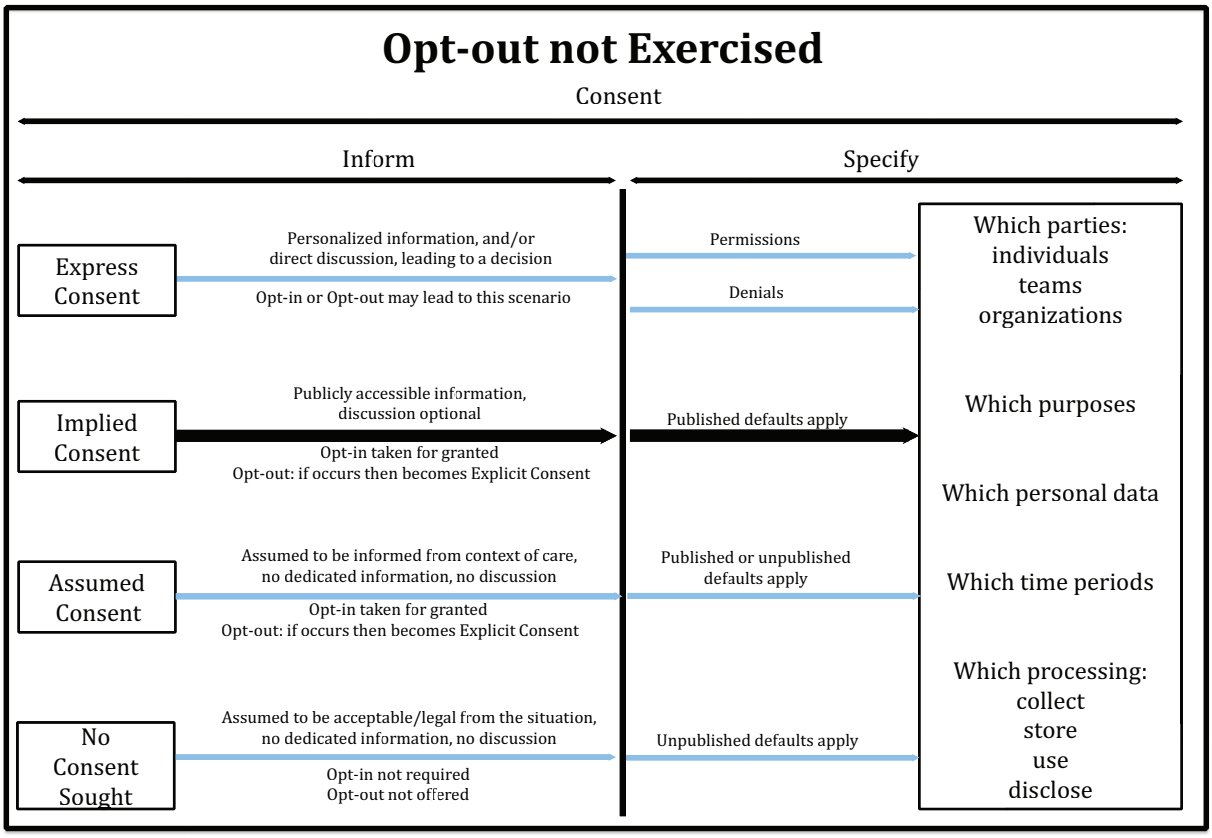

Figure B.1 — Consent framework diagram – Opt-out is not exercised (Implicit or Implied Consent)

Scenario 2 – the patient wishes to opt out, which they do so by engaging with their general practitioner with whom a discussion takes place followed by the exercising of that choice.

Thus, the patient does not want their identifiable data to flow but has no choice on the flow of the related clinical data. This provides two separate applications of the consent model for a) the clinical data and for b) the identifiable data. Consent model application – clinical data – No Consent is sought as it is not required.

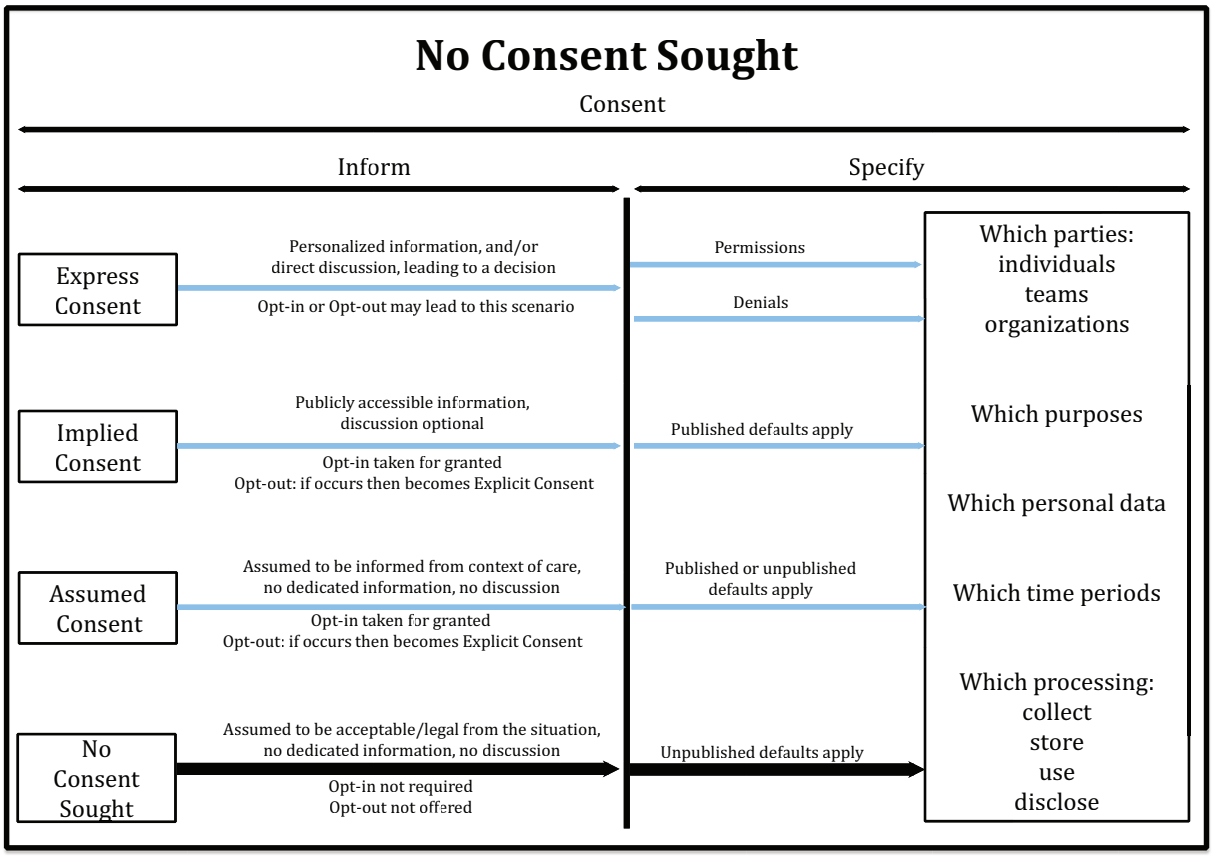

Figure B.2 — Consent model diagram – Clinical data – No Consent is sought as it is not required

Consent model application – identifiable data – Opt-out exercised by use of Explicit Consent, where the specific consent is a Denial.

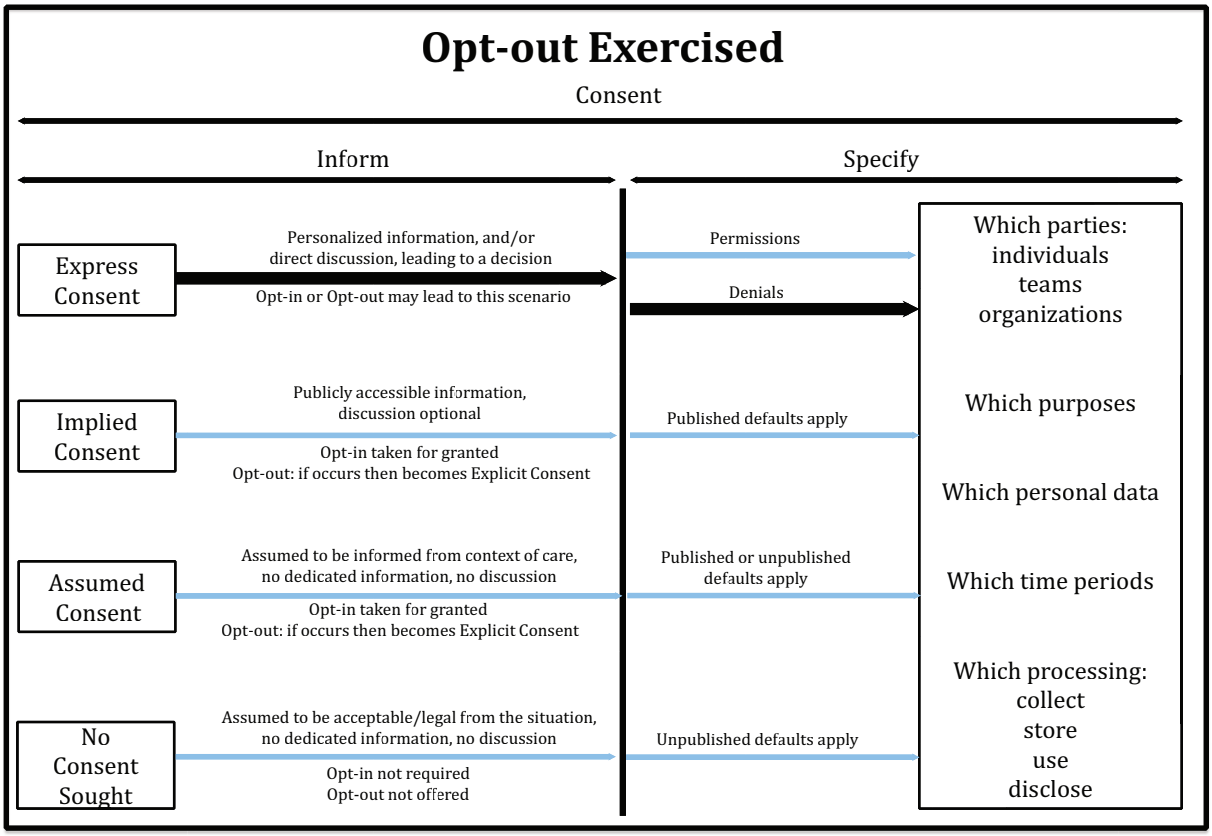

Figure B.3 — Consent model diagram – Identifiable data – Opt-out is exercised

Bibliography

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

[2] ISO/IEC 10181-3:1996, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Access control framework — Part 3*

[3] ISO 13606-4:2008, *Health informatics — Electronic health record communication — Part 4: Security*

[4] ISO/TS 14441:2013, *Health informatics — Security and privacy requirements of EHR systems for use in conformity assessment*

[5] ISO/TS 21298:2008, *Health informatics — Functional and structural roles*

[6] ISO 22600:2014, *Health informatics — Privilege management and access control — Parts 1–3*

[7] ISO 22857:2013, *Health informatics — Guidelines on data protection to facilitate trans-border flows of personal health data*

[8] ISO/TS 25237:2008, *Health informatics — Pseudonymization*

[9] ISO 27799:2008, *Health informatics — Information security management in health using ISO/IEC 27002*

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™