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.