TECHNICAL SPECIFICATION

ISO/TS 17975

Second edition
2022-11

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 17975:2022(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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 of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 215, *Health informatics*.

This second edition cancels and replaces the first edition (ISO/TS 17975:2015), which has been technically revised.

The main changes are as follows:

— editorial revision;

— Clause 2 and the bibliography have been updated.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document defines several frameworks for informational consent in healthcare. These are frequently used by organizations who wish to obtain agreement from individuals in order to process their personal health information.

NOTE 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.

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 document covers situations involving informational consent in routine healthcare service delivery. There can 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.

In order to align with internationally accepted privacy principles, this document 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 of Helsinki 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. 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 document 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 makes 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 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, 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 document describes the various informational consent frameworks and identifies the core principles that are common to all frameworks.

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 document is applicable regardless of frequency or scale of use and disclosure. However, it does assert that every 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 requiring explicit consent because it is a direct and necessary purpose associated with healthcare service delivery. In this case, the business activity for which the data is 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 required in this document and implementers are therefore free to apply this 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 can 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 applicable requirements.

Inter-relationship with other standards

This document can be used as a semantic complement to the ISO 22600 series and ISO 13606-4, both of which provide formal architectural and modelled representations of policies but do not themselves include requirements for consent.

ISO 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 must 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. Based on ISO 23903, the ISO 22600 series defines the necessary policy ontology, and ISO 21298 is a vocabulary for functional and structural roles.

ISO/TS 14441 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 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 13606-4 defines a policy model for requesting and providing EHR extracts (i.e. for one particular case to which this document might be applied). ISO 13606-4 also defines a concepts related to the sensitivity of EHR data.

ISO 22857 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 ISO 22857 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 27799:2016 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 21298 defines functional and structural roles. These will support the instantiation of informational consent policies.

Health informatics — Principles and data requirements for consent in the collection, use or disclosure of personal health information

1 Scope

This document defines the set of frameworks of consent for the collection, use and/or disclosure of personal information by healthcare 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 healthcare services and the communication of electronic health records across organizational and jurisdictional boundaries.

This document is applicable to Personal Health Information (PHI).

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 document 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 document 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.

— specify what consent framework is applicable to a data classification or data purpose as this can vary according to law or policy, although an examples of implementation profile is provided in Annex B;

— 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 requirements on how individuals are informed of the specifics of the data, data sharing or data processing concerned;

— specify requirements on how consent itself or the specific activities of the consent process are recorded. Specific requirements on recording consent in EHR systems are given in ISO/TS 14441:2013, 5.3.2;

— specify any information security requirements, e.g. the use of encryption or specific forms of user authentication (see e.g. ISO 27799).

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 22600-3, *Health informatics — Privilege management and access control — Part 3: Implementations*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22600-3 and the following apply.

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

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

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

3.1
anonymization
process by which personal data is irreversibly altered in such a way that a *data subject* (3.6) can no longer be identified directly or indirectly, either by the data controller alone or in collaboration with any other party

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

[SOURCE: ISO 25237:2017, 3.2]

3.2
assumed consent
informational consent (3.17) 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* (3.6)

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

3.4
collection
obtention of data by any means including that of viewing them

3.5
consent
form of authorization, provided by the *individual* (3.16) to whom the data refers, that some information processing activity is or is not permitted