FINAL
DRAFT

TECHNICAL SPECIFICATION

ISO/DTS 14265

ISO/TC **215**

Secretariat: **ANSI**

Voting begins on:
2023-09-13

Voting terminates on:
2023-12-06

Health informatics — Classification of purposes for processing personal health information

Informatique de santé — Classification des besoins pour le traitement des informations de santé personnelles

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/DTS 14265:2023(E)

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 document 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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 215, *Health informatics*.

This second edition cancels and replaces the first edition (ISO/TS 14265:2011), which has been technically revised.

The main changes are as follows:

— the list of categories has been expanded to include subdivisions of the health service management, population and public health and research categories;

— other categories have been renamed to make their meaning and distinction from other categories more explicit;

— the categories have been organised within a hierarchy;

— the informative introduction has been shortened by removing explanatory material about basic data protection principles which were relatively novel at the time of the previous version but are now well understood across jurisdictions;

— the retained portions of the introduction have been made more crisp.

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

0.1 General

This document defines a set of categories of purpose for processing personal health information, to which specific purposes can be mapped if it is desirable to compare permitted and intended purposes for processing personal health data, or to determine if two or more permitted purposes are compatible. This document does not aim to present a comprehensive list of specific purposes, but that all specific purposes can be mapped to one or more of these categories. Although any specific purpose will usually map to one category, at times a purpose can be mapped to more than one category. The categories are not mutually-exclusive, and the mapping of a specific purpose might not always be unique to one category.

Categories of purpose to which specific purposes are mapped should be standardised to allow for consistent comparisons to be made, rules and guidelines developed, and people trained. Bodies that make data access decisions, sometimes known as data access bodies or data permit authorities, often specify rules for certain categories of purpose and can find this categorisation useful.

0.2 Rationale for this classification

A fundamental principle underlying the use of personal data, often codified in data protection legislation, is that it is necessary to formally specify the purpose for which data was originally collected and/or is permitted to be processed. Personal information is normally used only for the purpose or purposes for which it was collected or created, unless otherwise required or authorised by law, or with the explicit or implied consent of the data subject. All subsequent processing activities by the original data holder or others by whom the data is accessed needs to be for the same as, or compatible with, the original purpose.

Interoperability standards and common data models, and their progressive adoption by e-health programmes and clinical research platforms, are expanding the capacity for organizations to exchange personal health information, within and between countries. Large scale research and public health intelligence sharing are amongst the drivers for scaling up investments in these data infrastructures. Whilst it is common and desirable that much of the processing for analysis and knowledge generation utilises anonymised data or distributed (federated) querying mechanisms, it is sometimes necessary to use pseudonymised data if longitudinal or cross-organisational linkage is required; pseudonymised data is considered in some jurisdictions to be personal data. It can at times be difficult to robustly anonymise health data, for example in the case of rare disease patients, genetic and personalised medicine research, in which case the data can be considered still to be personal even if it has had many explicit identifiers removed.

In large distributed health data ecosystems, and even for point-to-point data sharing and access, it is important that personal data processing activities (collection, storage, access, analysis, linkage, communication, disclosure and retention) are compliant with the applicable permissions. For these data accesses and processing activities, policies need to be examined and the permissions they contain may need to be compared (brokered) between parties and systems. Ideally these policy negotiations should be capable of computable negotiation as often as possible, which can require the permissions including permitted purposes of use to be compared between a data provider and an intended data user.

Data protection legislation usually requires that permissions such as consent are granted for an intended purpose that often has to be quite precisely specified, such as when obtaining informed consent. When determining compatibility of purpose, either to arrive at a formal access/processing decision or to guide people who will make the final decision, it can be helpful to map a specific purpose to a more coarse-grained category.

0.3 Using purpose categories when communicating with the public

Many members of the public recognise the need to scale up the use and re-use of health data to improve the quality, connectivity and safety of healthcare to individuals, to improve the effectiveness of care pathways, to generate evidence to inform health service planning, public health and policy-making, for

research by public and private organisations including the development of drugs, devices, algorithms and personalised health services. However, a significant barrier to scaling up learning from health data is public concern about the uses made of their health data and their not understanding why their data might be used by different actors. It is important that the range of possible purposes can be communicated to the public in a manageable and understandable way. This set of purpose categories can serve as a useful framework for raising awareness and education for the public about the different ways in which health data might be used, and the same framework might serve as a basis for expressing public or patient preferences in a realistic way, if these can be exercised.

0.4 Alignment with other ISO standards

ISO 22600 (PMAC) defines an 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. Policy domains need also to specify which information properties each takes into account when making processing decisions. They need to specify a high level policy model containing those properties, to which all instances of that kind of policy must conform. ISO/EN 13606-4 defines such a policy model for requesting and providing EHR Extracts, i.e. for one particular use case.

Even if instances of policies conforming to the models defined in ISO 22600 or ISO/EN 13606-4 specify precise purposes of processing, mapping this to a standardised category of purpose provides a basic level of semantic interoperability and might support policy negotiations. It can also help to computably identify incompatibilities of purpose, even if the formal confirmation of compatibility requires the precise purposes to be compared by a decision maker.

This categorisation in accordance with this document can be used in conjunction with functional roles and data sensitivity classifications to complement and populate portions of a policy. Categories of purpose can also assist when developing role-based access models.

No particular technical approach for implementing policy services or policy bridging is implied in this document.

Health informatics — Classification of purposes for processing personal health information

1 Scope

This document defines a set of high-level categories of purposes for which personal health information can be processed: collected, used, stored, accessed, analysed, created, linked, communicated, disclosed or retained. This is in order to provide a framework for classifying the various specific purposes that can be defined and used by individual policy domains (e.g. healthcare organisation, regional health authority, jurisdiction, country) as an aid to the consistent management of information in the delivery of health care services and for the communication of electronic health records across organisational and jurisdictional boundaries.

Health data that have been irreversibly de-identified are outside the scope of this document, but since de-identification processes often includes some degree of reversibility, this document can also be used for disclosures of de-identified and/or pseudonymised health data whenever practicable.

This classification, whilst not defining an exhaustive set of purposes categories, provides a common mapping target to bridge between differing national lists of purpose and thereby supports authorised automated cross-border flows of EHR data.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

ISO and IEC maintain 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
authorisation
granting of rights, which includes the granting of access based on access rights

[SOURCE: ISO/IEC 2382:2015, 2126256, modified — Notes to entry deleted.]

3.2
consent
freely given specific and informed indication of a subject's agreement to personal data relating to him/her being processed

3.3
data subject
individual about whom personal data are recorded

[SOURCE: ISO 5127:2017, 3.13.4.01, modified — Note to entry deleted.]

3.4
de-identification
process of removing the association between a set of identifying data and the data subject

[SOURCE: ISO 25237:2017, 3.20]

3.5
disclosure
divulging of or provision of access to data

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.

[SOURCE: ISO 25237:2017, 3.22]

3.6
personal data
data relating to an identified or identifiable individual

[SOURCE: ISO 5127:2017, 3.1.10.14, modified — Notes to entry deleted.]

3.7
personal health information
information about an identifiable person that relates to the physical or mental health of the individual

Note 1 to entry: To provision of health services to the individual and that may include:

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 anonymized, the identity of the individual who is the subject of the information cannot be ascertained from the information.

[SOURCE: ISO 27799: 2016, 3.8]

3.8
policy
set of rules related to a particular purpose

Note 1 to entry: A rule can be expressed as an obligation, an authorization, a permission or a prohibition.

[SOURCE: ISO 19101-2:2018, 3.29, modified — Note 1 to entry added]

3.9
processing
operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

4 Abbreviated terms

EHR electronic health tecord

PHI personal health information

5 Conformance

A policy domain conforms to this document if every agreed purpose for which the processing of PHI is permitted within that domain is published in a form that is categorised according to the classification in Clause 6. It is not a requirement that every category of purpose defined in this document has a correspondence with purposes supported within a conforming policy domain.

6 Classification of purposes for processing personal health information

The classification terms and descriptions of categories of purpose for processing PHI are given in Table 1, with coded values for each category. Examples of more specific purposes corresponding to these categories are given in Annex A.

The vocabulary identification for this list of coded values shall be referenced by the following OID.

Vocabulary Identification: iso (1) standard (0) Classification of Purposes for processing personal health information (14265) Terminology for classifying purposes for processing personal health information (1) and then the code shown in the first column in Table 1.

EXAMPLE "Managing outbreaks" has the OID code 1.0.14265.3.1

Table 1 — Code and corresponding classification term and description

Code	Heading	Category	Description
1.0	Person centred care		Processing that directly or indirectly contributes to the health and care of an individual, the data subject
1.1		Providing direct health and care services to individuals and families	Processing relating to the provision of health and care services to an individual, including documenting health status and health relevant information
1.2		Enabling continuity of care	Purposes relating to the interaction between health and care professionals in support of the health of and care to an individual
1.3		Providing and monitoring personal health, personalised care and wellness	Purposes that enable equipping and supporting an individual to manage their own health and care, including reviewing the data arising from self-provided care
1.4		Providing support and management to direct health and care services	Purposes that enable health and care services to be provided efficiently and safely in support of an individual or family
1.5		Supporting individuals with activities requiring trusted health information	Processing on behalf of and/or at the request of the data subject where health related information supports non-healthcare purposes
1.6		Obtaining evidence for care reimbursement and billing	Purposes initiated by the provider of health and care services to an individual in order to obtain authorisation for or reimbursement of services

Table 1 *(continued)*

Code	Heading	Category	Description
2.0	Health service management and quality assurance		Processing that utilises the personal data of an individual in order to monitor and improve the quality, safety and equity of health and care provision to a broad range of individuals
2.1		Quality monitoring	Measuring the quality of health and care services, measuring and improving health outcomes
2.2		Optimising care pathways	Assessing and comparing quality of care and outcomes using different models of care delivery and treatment
2.3		Safety monitoring	Measuring patient safety, reviewing adverse incidents, and assessing the effectiveness of safeguards
2.4		Product monitoring	Measuring the safety and effectiveness of health and care, or medicinal products and medical devices
2.5		Service planning	Obtaining evidence for health and care service planning and strategy
2.6		Capacity building	Developing and assessing the skills and competences required to grow health service capacity
3.0	Population and public health		Processing personal health data to track public health concerns, manage public health risks to individuals and populations, and develop effective strategies
3.1		Managing outbreaks	Detecting and managing outbreaks, controlling disease spread and mitigating adverse environmental issues
3.2		Managing public health programmes	Designing, running and evaluating screening, prevention and occupational health programmes
3.3		Targeting health needs	Assessing and monitoring unmet health and care needs
3.4		Public health strategy	Using personal health data to derive evidence for public health planning and strategy
3.5		Population health assessment	Assessing compound health and specific health patterns in a group of identified individuals
3.6		Population health strategies	Developing and monitoring strategies of specified health matters concerning individuals based on population health assessments
4.0	Clinical research		The design and conduct of clinical trials, real world data studies and other forms of knowledge generation that involve the processing of personal health data
4.1		Epidemiology	Understanding diseases, causes, prevention and treatment
4.2		Health technology innovation	Developing and testing new therapies, diagnostics, algorithms and health technology
4.3		Health services innovation	Evaluating, developing and optimising care pathways, health outcomes and self-care strategies
D4		Health systems evaluations	Measuring and improving the effectiveness and efficiency of health and care delivery
5.0	Education and training		Processing personal health data to develop education and training materials, to deliver teaching or to evaluate learning
5.1		Health professional education	Education, professional development and assessments of health and care professionals
5.2		Health related education	Education of health-related personnel, clinical research personnel, data scientists, managers