~~ISO/DTS 14265~~

~~ISO TC 215/WG 4~~

ISO/DTS 14265

ISO/TC 215

Secretariat: ~~ANSI~~ANSI

~~Health informatics — Classification of purposes for processing personal health information~~

~~*Élément introductif — Élément central — Élément complémentaire*~~

~~DTS~~ Date: 2023-08-30

Health informatics — Classification of purposes for processing personal health information

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

Document type: **Error! Reference source not found.**

Document subtype: **Error! Reference source not found.**

Document stage: **Error! Reference source not found.**

Document language: **Error! Reference source not found.**

FDIS stage

~~Warning for WDs and CDs~~

~~This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.~~

~~Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.~~

Document type: **Error! Reference source not found.**

Document subtype: **Error! Reference source not found.**

Document stage: **Error! Reference source not found.**

Document language: **Error! Reference source not found.**

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

Published in Switzerland

Contents

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~~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).

~~Attention is drawn~~ISO draws attention to the possibility that ~~some of~~ the ~~elements~~implementation of this document may ~~be~~involve the ~~subject~~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. ~~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~~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~~, as specified here,~~ 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 ~~could~~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 ~~could~~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

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 ~~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~~https://www.iso.org/obp

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