

Dit document mag slechts op een stand-alone PC worden geïnstalleerd. Gebruik op een netwerk is alleen toestaan als een aanvullende licentieovereenkomst voor netwerkgebruik met NEN is afgesloten.
This document may only be used on a stand-alone PC. Use in a network is only permitted when a supplementary license agreement for us in a network with NEN has been concluded.



Nederlandse praktijkrichtlijn

NPR-ISO/TS 14265

(en)

Health Informatics – Classification of purposes
for processing personal health information
(ISO/TS 14265:2011, IDT)

ICS 35.240.80
november 2011

Als Nederlandse praktijkrichtlijn is aanvaard:

- ISO/TS 14265:2011, IDT

Normcommissie 303006 "Informatievoorziening in de zorg"



THIS PUBLICATION IS COPYRIGHT PROTECTED

DEZE PUBLICATIE IS AUTEURSRECHTELIJK BESCHERMD

Apart from exceptions provided by the law, nothing from this publication may be duplicated and/or published by means of photocopy, microfilm, storage in computer files or otherwise, which also applies to full or partial processing, without the written consent of the Netherlands Standardization Institute.

The Netherlands Standardization Institute shall, with the exclusion of any other beneficiary, collect payments owed by third parties for duplication and/or act in and out of law, where this authority is not transferred or falls by right to the Reproduction Rights Foundation.

Auteursrecht voorbehouden. Behoudens uitzondering door de wet gesteld mag zonder schriftelijke toestemming van het Nederlands Normalisatie-instituut niets uit deze uitgave worden veelevoudigd en/of openbaar gemaakt door middel van fotokopie, microfilm, opslag in computerbestanden of anderszins, hetgeen ook van toepassing is op gehele of gedeeltelijke bewerking.

Het Nederlands Normalisatie-instituut is met uitsluiting van ieder ander gerechtigd de door derden verschuldigde vergoedingen voor veelevoudiging te innen en/of daartoe in en buiten rechte op te treden, voor zover deze bevoegdheid niet is overgedragen c.q. rechtens toekomt aan de Stichting Reprorecht.

Although the utmost care has been taken with this publication, errors and omissions cannot be entirely excluded. The Netherlands Standardization Institute and/or the members of the committees therefore accept no liability, not even for direct or indirect damage, occurring due to or in relation with the application of publications issued by the Netherlands Standardization Institute.

Hoewel bij deze uitgave de uiterste zorg is nagestreefd, kunnen fouten en onvolledigheden niet geheel worden uitgesloten. Het Nederlands Normalisatie-instituut en/of de leden van de commissies aanvaarden derhalve geen enkele aansprakelijkheid, ook niet voor directe of indirecte schade, ontstaan door of verband houdend met toepassing van door het Nederlands Normalisatie-instituut gepubliceerde uitgaven.

Copyright
Preview

Health informatics — Classification of purposes for processing personal health information

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



Copyrighted
Preview



COPYRIGHT PROTECTED DOCUMENT

© ISO 2011

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword	iv
0 Introduction.....	v
0.1 Rationale	v
0.2 Background.....	v
0.3 Context for defining data purposes.....	vi
1 Scope.....	1
2 Terms and definitions	2
3 Abbreviated terms	4
4 Conformance	4
5 Context	4
6 Terminology for classifying purposes for processing personal health information	5
Annex A (informative) Examples	7
Bibliography.....	13

Copyright
 Preview

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of normative document:

- an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;
- an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.

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.

ISO/TS 14265 was prepared by Technical Committee ISO/TC 215, *Health informatics*.

0 Introduction

0.1 Rationale

A fundamental principle underlying the use of personal health data is that it is essential to know the purposes for which data was originally collected and that all subsequent processing activities be the same as, or consistent with, the original purpose. This principle, when applied in conjunction with a standardized list of purposes, forms the foundation for a correspondence of permitted purpose between different users, systems, organizations or policy domains who might need to share personal health information.

Interoperability standards, and their progressive adoption by e-health programmes, are expanding the capacity for organizations to exchange health data. For this to occur on a wide scale, the majority of decisions regarding requests for health data will need to take place automatically. In order that data processing activities (collection, storage, access, analysis, linkage, communication, disclosure and retention) are appropriate, it is important that policies are defined in fully computable ways that are themselves interoperable. Interoperable policies will enable requests between heterogeneous systems and services to be evaluated consistently. In order for automatic processing policies to be defined and operationalized, it is important that governance structures, processes and rules are applied to the design of information and information technology at an enterprise or inter-enterprise level through a number of administrative mechanisms. These mechanisms include enterprise architecture/frameworks, standards, strategy, procedures, laws, regulations, principles and policy, and include operational controls such as committees, budgets, plans, and responsibility agreements (e.g. information sharing agreements, service level agreements and contracts). It is recognized that not all disclosures will take place automatically, and that individual (human) decisions will at times be made, taking policies and governance arrangements into account.

For ethical and legal reasons, it is normally the case that information is used only for the purpose for which it was collected or created. This purpose can be specified explicitly and consented to. Consent to use data for a particular purpose can also be implied, although it is almost always a requirement that the purposes be declared.

Where data are intended for further and different purposes, a new purpose can require a new consent. 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 new consent. Knowing the purpose for which access to information is intended is essential in order to determine if access to data for processing activities are appropriate.

Increasingly, this problem has become not only one of determining that a user has permission to access particular items of information but also that the user has permission to use them for a specified purpose. It is therefore essential to ensure that the context within which access and use is asserted is the correct one. Purpose (or use, purpose of use, or context of use) when clearly defined, helps to ensure that access to protected information items is granted to properly authorized users under a specific, appropriate and unambiguous policy. The explicit declaration of intended purpose prior to being granted access also helps to ensure that users understand that such access does not imply that use is also permitted for other undeclared, inconsistent purposes. Purpose of use helps bring clarity to situations where there are multiple and potentially conflicting contextually sensitive policies for identical users' access to identical information items.

0.2 Background

ISO/TS 22600-1 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 needs also to specify which information properties they wish to take 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/TS 14265:2011(E)

ISO/TS 13606-4 defines such a policy model for requesting and providing electronic health record (EHR) extracts i.e. for one particular use case.

Even if two or more parties share a common policy model, this is not sufficient to support policy bridging (automated inter-policy negotiation): the terms used for each property within the shared policy model need to be mutually understood between requesters and providers of health information. In other words, the properties and terms used in the request (collection) policy need to have a computable correspondence with the terms and policies of the recipient's disclosure policy in order for an automated access decision to be made.

Historically, data uses have been categorized as Primary and Secondary. Because these are relative terms, they only have meaning when one knows the perspective of the user. This then has the further problem of giving the impression that some purposes are more important than others when it could be argued that the secondary use of health information for the benefit of society is an important purpose. It is therefore proposed that those terms be replaced with explicit and neutral but informative labels. Data collected for inclusion in an EHR is initially collected for the purpose of care, although it may be subsequently used for other purposes. Explicitly stating those uses rather than using a generic label such as "secondary use" will improve communications, transparency and support appropriate use of data.

This Technical Specification is intended to be a semantic complement to ISO/TS 22600-1 and ISO/TS 13606-4, which both provide formal architectural and modelled representations of policies, but do not themselves include a vocabulary for purpose. However, it is not a requirement for a jurisdiction to adopt either of these two specifications in order to use this classification of purposes.

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

0.3 Context for defining data purposes

Defining data purposes is the critical first step in subsequent activities of data collection and various kinds of processing. Only once the intended purpose of data is known is it possible to assess if access to data or other processing activities are appropriate, for example:

- what is appropriate to collect,
- how it should be used,
- to whom it should be disclosed, and
- for how long it should be retained.

When making an access decision, authorization is a separate axis from purpose, and as such is not included in this classification. Authorization for collection, use or disclosure will be different in different jurisdictions, countries or situations, and will depend upon the environment within which the data are used. Authorization can be obtained in a number of ways, e.g. by consent, by law, by policy. In any given environment, different uses can require different authority. For example, the use of data for research might require explicit consent of the individual, but use of data for the person's direct care might rely upon implied consent. For data to be used in an investigation, legal authority and proof of a subpoena to force its disclosure and permit its collection might be required. Authority is an additional control over data collection or disclosure so that it can be made available for use (to collect, use or disclose data without sufficient or appropriate authorization might create legal risks or other risks for the user).

When first collected or created, data have some purposes which ought to be defined and explicitly stated, unless there are well recognized grounds for regarding the intended purposes as transparent within the context of capture, and if the data subject is expected to be adequately aware of this (i.e. if there is implied informed consent based on what the data subject knows or should have known). Later, when the data are requested for use within an organization or team, or disclosed for use by external parties, the requester might

intend a different purpose. In jurisdictions where a new or additional purpose is permitted (in other words, where a new purpose is assigned to data after its collection), it might be necessary to compare the new purpose with the original authorized purpose, in order to decide if the new purpose is permitted.

In jurisdictions where it is permitted to use data collected for one purpose for a new purpose, before any access is granted it might be necessary to compare the two purposes (the original consented or otherwise authorized purpose and the new intended purpose for which the access or disclosure is made) in order to decide if the new use is permitted.

After accessing data intended for some purpose related to use or disclosure, that purpose 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 purpose that is declared and documented.

A justifiable purpose ought to exist on the part of those who seek to collect data. In some circumstances, as is the case in some investigations, the requestor might have the authority to demand information without providing a purpose.

Collection of data, whether directly from the individual or indirectly from another body, ought to limit data collected to that which is required to satisfy a justifiable need on the part of the collecting organization ("collection limitation"). Justification of a need forms part of the governance and high level policy setting of an organization or jurisdiction.

Defined purpose also indicates the context for the collection of informed consent. Informed consent is a mechanism whereby a person is able to control the collection, use and/or disclosure of their data; it is important that the consent mechanism allows the data subject to make a free and informed choice. The reference to "knowledge" in the phrase "knowledge and consent" refers to the data subject's right to know about the uses to which the data will be put after they are collected.

In some cases, such as when data are sought for purposes under law, once disclosed, the data are then subject to the permitted uses of the recipient, e.g. in a legal investigation. What matters when data are disclosed as required or permitted by law, or permitted by agreement, is the legal authority of the body disclosing the data. However, it might also be necessary that data be disclosed only for a specific purpose.

This Technical Specification does define data purposes, but it is not meant to provide a comprehensive listing of purposes for which a legal obligation to disclose exists. Legal obligation to disclose, report or communicate data overrides the requirement to match the purpose for which data are held with the purposes to which the recipient uses the information. The recipient is legally permitted to demand and to receive the information without having to declare a purpose, without having to fit in with the existing purposes, or having to obtain consents under which data are held.

At times, it might be important to enforce policies on the recipient of a data disclosure (the indirect collector) to ensure that the recipient only uses the data for the declared purpose. Label-based access controls, or governance-based access controls, can allow the legislated or policy-based permissions to be applied at the technical level to help enforce this.

Data purposes or specific uses may or may not require identifiable data. Some data purposes might require the use of identifiable, de-identified, anonymous, pseudonymous or aggregate data. Although this Technical Specification will not seek to dictate which purposes may or may not use identifiable data, it is commonly understood that where identity is not required it should not be disclosed. Identity is most often required when the purpose of use is to the benefit of the individual data subject, as when the data subject is also a subject of care. The de-identification, anonymization, or pseudonymization of data may be applied as a confidentiality control or condition of use, just as appropriate authority may be applied as a condition of collection, use or disclosure. This in turn means that just as de-identification may be applied as a condition of use, a defined data purpose may be a requirement for the use of even de-identified or anonymized data according to the policy or law of a given jurisdiction.

Where a unique identifier is required to enable linkage to other data sources, best practice indicates that a genuine pseudo-identifier be used, although it is still common practice to use identifiable data to enable such linkage where a robust mechanism for using pseudo-identifiers is not in place across the relevant data sources. ISO/TS 25237 is the basis for pseudo-identifier management.

Bestelformulier

NEN

Stuur naar:

NEN Standards Products & Services
t.a.v. afdeling Klantenservice
Antwoordnummer 10214
2600 WB Delft

NEN Standards Products & Services

Postbus 5059
2600 GB Delft

Vlinderweg 6
2623 AX Delft

T (015) 2 690 390
F (015) 2 690 271

www.nen.nl/normshop

Ja, ik bestel

__ ex. NPR-ISO/TS 14265:2011 en Medische informatica - Classificatie van doeleinden voor de verwerking van persoonlijke medische gegevens € 79.70

Wilt u deze norm in PDF-formaat? Deze bestelt u eenvoudig via www.nen.nl/normshop

Gratis e-mailnieuwsbrieven

Wilt u op de hoogte blijven van de laatste ontwikkelingen op het gebied van normen, normalisatie en regelgeving? Neem dan een gratis abonnement op een van onze e-mailnieuwsbrieven. www.nen.nl/nieuwsbrieven

Retourneren

Fax: (015) 2 690 271
E-mail: klantenservice@nen.nl
Post: NEN Standards Products & Services,
t.a.v. afdeling Klantenservice
Antwoordnummer 10214,
2600 WB Delft
(geen postzegel nodig).

Gegevens

Bedrijf / Instelling _____

T.a.v. _____ O M O V

E-mail _____

Klantnummer NEN _____

Uw ordernummer _____ BTW nummer _____

Postbus / Adres _____

Postcode _____ Plaats _____

Telefoon _____ Fax _____

Factuuradres (indien dit afwijkt van bovenstaand adres)

Postbus / Adres _____

Postcode _____ Plaats _____

Datum _____ Handtekening _____

Voorwaarden

- De prijzen zijn geldig tot 31 december 2016, tenzij anders aangegeven.
- Alle prijzen zijn excl. btw, verzend- en handelingskosten en onder voorbehoud bij o.m. ISO- en IEC-normen.
- Bestelt u via de normshop een pdf, dan betaalt u geen handeling en verzendkosten.
- Meer informatie: telefoon (015) 2 690 391, dagelijks van 8.30 tot 17.00 uur.
- Wijzigingen en typfouten in teksten en prijsinformatie voorbehouden.
- U kunt onze algemene voorwaarden terugvinden op: www.nen.nl/leveringsvoorwaarden.