SLOVENSKI STANDARD
SIST EN ISO 25237:2017

01-maj-2017

Zdravstvena informatika - Psevdonimizacija (ISO 25237:2017)

Health informatics - Pseudonymisation (ISO 25237:2017)

Medizinische Informatik - Pseudonymisierung (ISO 25237:2017)

Informatique de santé - Pseudonymization (ISO 25237:2017)

Ta slovenski standard je istoveten z: **EN ISO 25237:2017**

ICS:

35.240.80	Uporabniške rešitve IT v zdravstveni tehniki	IT applications in health care technology

SIST EN ISO 25237:2017 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO 25237

January 2017

ICS 35.240.80

English Version

Health informatics - Pseudonymization (ISO 25237:2017)

Informatique de santé - Pseudonymisation (ISO 25237:2017)

Medizinische Informatik - Pseudonymisierung (ISO 25237:2017)

This European Standard was approved by CEN on 14 December 2016.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

European foreword

This document (EN ISO 25237:2017) has been prepared by Technical Committee ISO/TC 215 “Health informatics” in collaboration with Technical Committee CEN/TC 251 “Health informatics” the secretariat of which is held by NEN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by July 2017, and conflicting national standards shall be withdrawn at the latest by July 2017.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO 25237:2017 has been approved by CEN as EN ISO 25237:2017 without any modification.

Type de document : Norme européenne
Sous-type de document :
Stade du document : Publication / Adoption
Langue du document : E

Y:\STD_MGT\STDDEL\PRODUCTION\Standards\00251\316\64_e_stf.doc STD Version 2.5a

INTERNATIONAL STANDARD

ISO 25237

First edition
2017-01

Health informatics — Pseudonymization

Informatique de santé — Pseudonymisation

Reference number
ISO 25237:2017(E)

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 World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/TC 215, *Health informatics*.

Introduction

Pseudonymization is recognized as an important method for privacy protection of personal health information. Such services may be used nationally, as well as for trans-border communication.

Application areas include, but are not limited to:

— indirect use of clinical data (e.g. research);

— clinical trials and post-marketing surveillance;

— pseudonymous care;

— patient identification systems;

— public health monitoring and assessment;

— confidential patient-safety reporting (e.g. adverse drug effects);

— comparative quality indicator reporting;

— peer review;

— consumer groups;

— field service.

This document provides a conceptual model of the problem areas, requirements for trustworthy practices, and specifications to support the planning and implementation of pseudonymization services.

The specification of a general workflow, together with a policy for trustworthy operations, serve both as a general guide for implementers but also for quality assurance purposes, assisting users of the pseudonymization services to determine their trust in the services provided. This guide will serve to educate organizations so they can perform pseudonymization services themselves with sufficient proficiency to achieve the desired degree of quality and risk reduction.

Health informatics — Pseudonymization

1 Scope

This document contains principles and requirements for privacy protection using pseudonymization services for the protection of personal health information. This document is applicable to organizations who wish to undertake pseudonymization processes for themselves or to organizations who make a claim of trustworthiness for operations engaged in pseudonymization services.

This document

— defines one basic concept for pseudonymization (see Clause 5),

— defines one basic methodology for pseudonymization services including organizational, as well as technical aspects (see Clause 6),

— specifies a policy framework and minimal requirements for controlled re-identification (see Clause 7),

— gives an overview of different use cases for pseudonymization that can be both reversible and irreversible (see Annex A),

— gives a guide to risk assessment for re-identification (see Annex B),

— provides an example of a system that uses de-identification (see Annex C),

— provides informative requirements to an interoperability to pseudonymization services (see Annex D), and

— specifies a policy framework and minimal requirements for trustworthy practices for the operations of a pseudonymization service (see Annex E).

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 27799, *Health informatics — Information security management in health using ISO/IEC 27002*

3 Terms and definitions

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

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

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

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

3.1
access control
means of ensuring that the resources of a data processing system can be accessed only by authorized entities in authorized ways

[SOURCE: ISO/IEC 2382:2015, 2126294]

3.2
anonymization
process by which *personal data* (3.37) is irreversibly altered in such a way that a data subject 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 may be difficult to obtain.

[SOURCE: ISO/IEC 29100:2011, 2.2, modified.]

3.3
anonymized data
data (3.14) that has been produced as the output of an *anonymization* (3.2) process

[SOURCE: ISO/IEC 29100:2011, 2.3, modified.]

3.4
anonymous identifier
identifier (3.27) of a person which does not allow the *identification* (3.26) of the *natural person* (3.34)

3.5
authentication
assurance of the claimed identity

3.6
attacker
person deliberately exploiting vulnerabilities in technical and non-technical security controls in order to steal or compromise information systems and networks, or to compromise availability to legitimate users of information system and network resources

[SOURCE: ISO/IEC 27033-1:2015, 3.3]

3.7
ciphertext
data (3.14) produced through the use of encryption, the semantic content of which is not available without the use of cryptographic techniques

[SOURCE: ISO/IEC 2382:2015, 2126285]

3.8
confidentiality
property that *information* (3.29) is not made available or disclosed to unauthorized individuals, entities or processes

[SOURCE: ISO 7498-2:1989, 3.3.16]

3.9
content-encryption key
cryptographic key used to encrypt the content of a communication

3.10
controller
natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the *processing of personal data* (3.40)

3.11
cryptography
discipline which embodies principles, means and methods for the transformation of *data* (3.14) in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use

[SOURCE: ISO 7498-2:1989, 3.3.20]

3.12
cryptographic algorithm
<cipher> method for the transformation of *data* (3.14) in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use

3.13
cryptographic key management
key management
generation, storage, distribution, deletion, archiving and application of *keys* (3.31) in accordance with a *security policy* (3.46)

[SOURCE: ISO 7498-2:1989, 3.3.33]

3.14
data
reinterpretable representation of *information* (3.29) in a formalized manner suitable for communication, interpretation or processing

Note 1 to entry: Data can be processed by humans or by automatic means.

[SOURCE: ISO/IEC 2382:2015, 2121272]

3.15
data integrity
property that *data* (3.14) has not been altered or destroyed in an unauthorized manner

[SOURCE: ISO 7498-2:1989, 3.3.21]

3.16
data linking
matching and combining *data* (3.14) from multiple databases

3.17
data protection
technical and social regimen for negotiating, managing and ensuring informational *privacy* (3.39), and security

3.18
data subject
person to whom *data* (3.14) refer

3.19
decryption
process of converting encrypted *data* (3.14) back into its original form so it can be understood

3.20
de-identification
general term for any process of reducing the association between a set of identifying *data* (3.14) and the *data subject* (3.18)

3.21
directly identifying data
data (3.14) that directly identifies a single individual

Note 1 to entry: Direct identifiers are those data that can be used to identify a person without additional information or with cross-linking through other information that is in the public domain.