TECHNICAL REPORT

ISO/TR 18638

First edition
2017-06

Health informatics — Guidance on health information privacy education in healthcare organizations

Informatique de santé — Composantes éducatives destinées à garantir la confidentialité des informations relatives à la santé

Reference number
ISO/TR 18638:2017(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 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 the following URL: www.iso.org/iso/foreword.html.

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

Introduction

Health information privacy concerns need to be addressed with the expanding adoption of health information technology (HIT) including the use of electronic health record (EHR) systems. Both the increasingly legislated environment around privacy and the increasing need for information sharing between patients, providers, payers, researchers and administrators contribute to the growing need for information privacy education in the healthcare sector. In spite of increasing awareness of and sensitivity to patient privacy, there are no guidelines or standardization for education on privacy of the healthcare information within healthcare organizations.

The purpose of this document is to describe the essential educational components recommended to ensure health information privacy in a healthcare organization. This document describes the concepts of health information privacy, the components of a privacy education program for healthcare organizations and basic health information privacy educational content that can be applied to various jurisdictions.

This document provides guidance for healthcare organizations for establishing and improving the health information privacy education for their workforce.

Annex A provides the list of standards published by ISO/TC 215 that may be used to develop privacy education in healthcare organizations as they convey specific content and approach health information privacy protection.

Health informatics — Guidance on health information privacy education in healthcare organizations

1 Scope

This document specifies the essential educational components recommended to establish and deliver a privacy education program to support information privacy protection in healthcare organizations. The primary users of this document are those responsible for planning, establishing and delivering healthcare information privacy education to a healthcare organization.

This document provides the components of privacy education within the context of roles and job responsibilities. It is the responsibility of the organization to define and apply privacy protection policies and procedures and, in turn, ensure that all staff in the healthcare organization understands their privacy protection responsibilities.

The scope of this document covers:

a) the concept of information privacy in healthcare;

b) the challenges of protecting information practices in the healthcare organization;

c) the components of a healthcare information privacy education program;

d) basic health information privacy educational content.

2 Normative references

There are no normative references for this document.

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
ability or means necessary to read, write, modify, or communicate data/information or otherwise make use of any system resources

[SOURCE: ISO/TR 18307:2001, 3.1]

3.2
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 17090-1:2013, 3.2.1]

3.3
anonymization
process by which *personal identifiable information (PII)* (3.21) is irreversibly altered in such a way that a *PII principal* (3.22) can no longer be identified directly or indirectly, either by the *PII controller* (3.23) alone or in collaboration with any other party

Note 1 to entry: See *pseudonymization* (3.33).

[SOURCE: ISO/IEC 27038:2014, 2.1, modified]

3.4
asset
anything that has value to the organization

Note 1 to entry: There are many types of assets, including:

a) information;

b) software, such as a computer program;

c) physical, such as computer;

d) services;

e) people, and their qualifications, skills and experience, and

f) intangibles, such as reputation and image.

[SOURCE: ISO/IEC 27000: 2014, 3.6]

3.5
audit
systematic, independent, documented process for obtaining records, statements of fact or other relevant information and assessing them objectively to determine the extent to which specified requirements are fulfilled

[SOURCE: ISO/IEC 29110-2-1:2015, 4.7]

3.6
availability
property of data or of resources being accessible and usable on demand by an authorized entity

Note 1 to entry: This is the definition relevant to use in computer security.

[SOURCE: ISO/TS 27790:2009, 3.10]

3.7
confidentiality
property of data that indicates the extent to which these data have not been made available or disclosed to unauthorized individuals, processes or other entities

[SOURCE: ISO/IEC 2382:2015, 2126249]

3.8
control
means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management or legal in nature

Note 1 to entry: Control is also used as a synonym for safeguard or countermeasure.

Note 2 to entry: Controls include any process, policy, device, practice, or other actions which modify risk.

Note 3 to entry: Controls may not always exert the intended or assumed modifying effect.

[SOURCE: ISO/IEC 27000:2016, 2.16]

3.9
education
knowledge, skill and understanding that you get from attending a school, college, university or vocational teaching

Note 1 to entry: The action or process of teaching someone especially in a school, college, or university.

Note 2 to entry: A field of study that deals with the methods and problems of teaching.

Note 3 to entry: Synonyms are learning, knowledge, literacy, scholarship and enlightenment

Note 4 to entry: Education (which is concept based) is different than *training* (3.39) (which is skill based).

3.10
healthcare
type of services is provided by professionals or paraprofessionals with an impact on health status

[SOURCE: ISO 27799:2016, 3.3]

3.11
healthcare organization
organization involved in the direct or indirect provision of healthcare services to an individual or to a population

[SOURCE: ISO 13606-1:2008, 3.33]

3.12
health professional
person who is authorized by a recognized body to be qualified to perform certain health duties

Note 1 to entry: The defined term is often “healthcare professional”.

[SOURCE: ISO 27799:2016, 3.5]

3.13
identifiable person
one who can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity

[SOURCE: ISO 22857:2013, 3.7]

3.14
information privacy
rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure and disposal of personal information

[SOURCE: ISO/TS 14441:2013, 3.26]

3.15
information security
protection of information from (accidental or intentional) unauthorized access, use, disclosure, disruption, modification or destruction

[SOURCE: ISO/TS 21547:2010, 3.2.24]

3.16
media
means by which information is perceived, expressed, stored or transmitted

EXAMPLE Audio, video, (animated) graphics, images, text.

Note 1 to entry: Medium (plural media).

[SOURCE: ISO/IEC 14478-1:1998, 3.2.2]

3.17
patient
subject of care consisting of one person

[SOURCE: ISO 13606-2:2008, 4.13]

3.18
personal information
information about an individual which can be used to identify that individual

Note 1 to entry: The specific information used for this identification will be that defined by national legislation.

Note 2 to entry: See *personal identifiable information (PII)* (3.21).

[SOURCE: ISO/IEC 27011:2008, 3.1.5]

3.19
personal health information
information about an identifiable person that relates to the physical or mental health of the individual

[SOURCE: ISO 27799:2016, 3.8]

3.20
personal health record
PHR
representation of information regarding or relevant to the health, including wellness, development, and welfare of a subject of care, which may be stand-alone or integrating health information from multiple sources, and for which the individual, or their authorized representative, manages and controls the PHR content and grants permissions for access by and/or sharing with other parties

[SOURCE: ISO/TR 14639-2:2014, 2.60]

3.21
personal identifiable information
PII
information about a person that can be used to identify that individual

Note 1 to entry: The specific information used for this identification will be that defined by national legislation.

Note 2 to entry: See *personal health information* (3.19) and *pseudonymization* (3.33).

[SOURCE: ISO/IEC 27011:2008, 3.1.5]

3.22
personal identifiable information principal
PII principal
person who granted/entrusted an organization with the ability to manage his/her PII

Note 1 to entry: See *pseudonymization* (3.33).

3.23
personal identifiable information controller
PII controller
person designated by an organization to control access to PII

Note 1 to entry: See *pseudonymization* (3.33).

3.24
policy
set of rules such as legal, political, organizational which can be expressed as obligations, permissions or prohibitions

Note 1 to entry: Adapted from ISO/TS 22600-1:2014, 3.13.

[SOURCE: ISO/TR 14639-1:2012]

3.25
privacy
freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual

[SOURCE: ISO/TS 27790:2009, 3.56]

3.26
privacy in healthcare
right of an individual to keep oneself and one's health information concealed or hidden from unauthorized access and view by others that rests on the principle of confidentiality between healthcare providers and patients

3.27
privacy breach
situation where *personal information* (3.18) is collected, accessed, used or disclosed in an unlawful manner or in violation of one or more relevant privacy policies

[SOURCE: ISO/TS 17975:2015, 3.26]

3.28
privacy manager
individual designated as a privacy official, who manages personal information directly or via another person as part of his/her duties, who is responsible for developing and implementing its privacy policies and procedures or a contact person or contact office responsible for receiving complaints and providing individuals with information on the healthcare organization's privacy practice

3.29
privacy protection
capacity to control when, how and to what degree information about oneself is communicated to others

3.30
privacy stakeholders
individuals involved in *privacy protection* (3.29) including *PII principal* (3.22), *PII controller* (3.23), *privacy manager* (3.28) and other defined by the national regulation

3.31
procedure
specified way to carry out an activity or a process

[SOURCE: ISO 30000:2009, 3.12]

3.32
provider
person or organization that is involved in or associated with delivery of health care to a subject of care, or caring for the well-being of a subject of care

Note 1 to entry: A provider in this context includes not only healthcare providers, but also those directly involved in the provision of services to patients.

Note 2 to entry: The defined term is often "healthcare professional". A convention has been adopted in this document whereby the term "healthcare" is abbreviated to "health" when used in an adjectival form. When used in a noun form, the word "care" is retained but as a separate word (e.g. delivery of health care).

[SOURCE: ISO/TS 27527:2010, 3.6]

3.33
pseudonymization
process applied to *personal identifiable information (PII)* (3.21) which replaces identifying information with an alias

Note 1 to entry: Synonym is reduction, masking.

Note 2 to entry: Pseudonymization can be performed either by *PII principals* (3.22) themselves or by *PII controllers* (3.23). See PII, PII principal and PII controller.

Note 3 to entry: Pseudonymization can be employed by PII principal to consistently use a resource or service without disclosing his/her identity to this resource or service (or between services), while still being held accountable for that use.

Note 4 to entry: Pseudonymization does not rule out the possibility that there might be (a restricted set of) privacy stakeholders other than the PII principle controller of the pseudonymized data which are able to determine the PII principal's identity based on the alias and data linked to it.

[SOURCE: ISO/IEC 29100:2011, 2.24]

3.34
review
verification of the suitability, adequacy and effectiveness of selection and determination activities, and the results of these activities, with regard to the fulfilment of specified requirements by an object of conformity assessment

[SOURCE: ISO/TS 14441:2013, 3.44]

3.35
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO 10377:2013, 2.16]

3.36
risk management
coordinated activities to direct and control an organization with regard to *risk* (3.35)

[SOURCE: ISO/TS 16901:2015, 3.32]

3.37
subject of care
one or more persons scheduled to receive, receiving, or having received a health service

[SOURCE: ISO/TS 18308:2011, 3.47]

3.38
threat
potential cause of an unwanted incident that may result in harm to a system or organization

3.39
training
process by which someone is taught the skills that are needed for an art, profession or job

Note 1 to entry: The action of teaching a person or animal a particular skill or type of behaviour.

Note 2 to entry: The action of undertaking a course of exercise and diet in preparation for a sporting event.

Note 3 to entry: Exercise, exercises, working out, conditioning.

Note 4 to entry: See *education* (3.9).

3.40
workforce
people who provide a service or labor to contribute to business or organizational outcomes

[SOURCE: ISO 30409:2016, 10.1]

4 Abbreviations

EHR	electronic health record
EN	European Norm (Standard)
EU	European Union
HIT	health information technology
ID	identification
ICT	information and communication technology
OECD	Organization for Economic Cooperation and Development
PHI	personal health information

5 Understanding information privacy in healthcare

5.1 General concept

The internet and emerging health information and communication technologies are changing the way that health professionals and the public gain access to health information, resulting in an expectation for the increased use of such information. Although personal health information is personally private data, such information may be used for public health, clinical research, medical education, policy making, legislation enforcement, accreditation and other purposes for the betterment of society. Healthcare organizations should develop a comprehensive approach to enable adequate protection of health information privacy for their patients. Workforce education regarding health information privacy should be an integral part of this approach including guidance on when and how health information should be protected with regards to the specific workforce roles.