PD ISO/TR 18638:2017

BSI Standards Publication

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

bsi.

National foreword

This Published Document is the UK implementation of ISO/TR 18638:2017.

Users of this Standard are advised that whilst TR 18638 provides generic guidance for the construct and delivery of health privacy education, UK health and care organizations may require additional training and awareness content in order to satisfy their obligations for information governance and data protection. It is recommended that health organizations wishing to deliver privacy education should also consult the latest available guidance from their appropriate national authority.

The UK participation in its preparation was entrusted to Technical Committee IST/35, Health informatics.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2017

ISBN 978 0 580 81871 4

ICS 35.240.80

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 July 2017.

Amendments/corrigenda issued since publication

Date	Text affected

PD ISO/TR 18638:2017

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)

COPYRIGHT PROTECTED DOCUMENT

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]