PD ISO/TR 17791:2013



BSI Standards Publication

Health informatics — Guidance on standards for enabling safety in health software

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of ISO/TR 17791:2013.

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.

© The British Standards Institution 2014. Published by BSI Standards Limited 2014

ISBN 978 0 580 77185 9

ICS 35.240.80

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

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 28 February 2014.

Amendments issued since publication

Date	Text affected

PD ISO/TR 17791:2013

TECHNICAL REPORT

ISO/TR 17791

First edition
2013-12-15

Health informatics — Guidance on standards for enabling safety in health software

Informatique de la santé — Conseils sur les normes de sécurité des logiciels de la santé

Reference number
ISO/TR 17791:2013(E)

© ISO 2013



COPYRIGHT PROTECTED DOCUMENT

© ISO 2013

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested 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**

Introduction ... **v**

1 Scope ... **1**

2 Terms and definitions ... **1**

3 Abbreviated terms ... **6**

4 Health software safety ... **6**
4.1 Health software safety incidents ... 6
4.2 Health software definitions ... 7
4.3 Towards safer health software ... 9
4.4 Health software lifecycle ... 9
4.5 How standards were selected for assessment ... 12
4.6 Standards assessed in this Technical Report ... 13
4.7 Risk management basis ... 15
4.8 Human factors basis ... 16
4.9 Granularity ... 17

5 Standards assessment and guidance ... **17**
5.1 Standards assessment ... 17
5.2 Standards assessed by lifecycle applicability and software granularity ... 31
5.3 Standards assessment overlap and gap analysis ... 33
5.4 Standards for enabling safety in health software — Implementation and use guidance ... 36

Annex A (informative) **Patient safety benefits arising from eHealth investments** ... **39**

Annex B (informative) **Standards analysis from a software lifecycle perspective** ... **40**

Annex C (informative) **Scope information of safety-relevant JTC 1 standards** ... **44**

Bibliography ... **47**

© ISO 2013 – All rights reserved

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 WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

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

© ISO 2013 – All rights reserved

Introduction

Improving patient safety

Patient safety is a major and worldwide concern in healthcare. As noted in the 2010 publication of ISO/TC215 *Summary Report from the Task Force on Patient Safety and Quality*, more than a decade had passed since the seminal publication in 1999 of "*To Err is Human: Building a Safer Health System*" by the Institute of Medicine (IOM).[1][2]

Since 1999, patient safety has been a consistent focus of deliberation and action at national and international levels. Best practices in patient safety have emerged with respect to reporting, root cause and risk analysis, prevention and mitigation. These practices have informed national and global approaches to improving patient safety. Education programs, national campaigns, local hospital priorities, adverse event and incident reporting tools, risk management training and clinician safety certification programs are all examples of ongoing efforts to foster a culture of heightened patient safety and quality improvement.

This focus on patient safety has spurred investments in inter-operable electronic health record (EHR) systems and decision support capabilities such as computerized physician order entry (CPOE). These investments ultimately seek to avoid if not mitigate the acknowledged occurrence of patient safety incidents due to causes such as drug-drug interactions.

Health informatics can both mitigate and introduce risks to patient safety

Health informatics and associated e-Health systems have significant potential to eliminate, reduce or mitigate documented threats to patient safety and quality of care (see Annex A) and are a current focus for major investment within healthcare systems.

Any major transformative technological change introduced into an industry, especially into a field as complex and life-altering as healthcare, will have both predictable and unexpected consequences. Unintended impacts can be both positive (e.g. by fostering new opportunities for clinicians to collaborate as users working with the new technology and thereby facilitating clinical process improvements) or negative (e.g. through introduction of new risks as a consequence of the design, implementation or use of the technology in busy clinical environments).

While the benefits of health informatics for patient safety are increasingly accepted, there are risks of inadvertent and adverse events caused by health software solutions and these risks are becoming more apparent. As increasingly sophisticated health software solutions are deployed that provide higher levels of decision support and integrate patient data between systems, across organizational lines, and across the continuum of care, the patient safety benefits increase along with the risks of software induced adverse events.

England's National Health Service (NHS) *Connecting for Health* IT program established a proactive safety incident management process to address software safety.[3] During the five year period from 2006 to 2010, 708 reported incidents were documented and investigated. Approximately 80 % of these incidents were found to pose some risk to patient safety (see Clause 4.1).

Standards enabling safety in health software – developments to date

The issue of safety in health software was first recognized within ISO/TC 215 in 2006, when work began on the following:

— ISO/TS 25238:2007, *Health informatics — Classification of safety risks from health software*, and

— ISO/TR 27809:2007, *Health informatics — Measures for ensuring patient safety of health software*.

ISO/TS 25238:2007 is targeted at the concept and requirements stages in the software lifecycle where it is necessary to understand in broad terms what a proposed system's risk class will be. While this Technical Specification includes example categories of severity and likelihood and a sample risk matrix

© ISO 2013 – All rights reserved

that may appear to have wider applicability, it is not the intention of the TS to apply these either to the design of health software products or to the mitigation of any identified risks to acceptable levels.

ISO/TR 27809:2007 provides an overview of the classification of health software products, a discussion of the options for control measures associated with such software, a reference to the risk classification scheme defined in ISO/TS 25238:2007, and the identification of national and international risk management standards.

The medical device community has supported software standards development for many years in IEC/TC 62 Subcommittee A (*Common aspects of electrical equipment used in medical practice*), ISO/TC 215 (Health informatics) and ISO/TC 210 (*Quality management and corresponding general aspects for medical devices*). Several other ISO and IEC technical committees such as the ISO/IEC JTC 1 Subcommittee 7 (*Software and systems engineering*) have been developing software and systems engineering standards since the late 1980s.

The medical device standards work to date has focused on defined medical devices' functionality and testing and has included standards on software as a medical device (In IEC 62304:2006, *Medical device software — Software life cycle processes, "software as a medical device"* is defined as a "software system that has been developed for the purpose of being incorporated into the medical device being developed or that is intended for use as a medical device in its own right"). Key standards developed or referenced for use for safety in medical devices and medical device software have included:

— ISO 13485:2003, *Medical devices — Quality management systems — Requirements for regulatory purposes*,

— ISO/TR 14969:2004, *Medical devices — Quality management systems — Guidance on the application of* ISO 13485:2003,

— IEC 62304:2006, *Medical device software — Software life cycle processes*,

— ISO 14971:2007, *Medical devices — Application of risk management to medical devices*, and

— IEC 80001-1:2010, *Application of risk management for IT networks incorporating medical devices, Part 1 — Roles, responsibilities and activities*.

The focus of these standards reflects the medical device industry's primary interest in the pre-market (i.e. design and development) aspects of the software product lifecycle, including software and medical devices that operate on a stand-alone basis. The recent addition of IEC 80001-1 is a sign of the growing attention towards the implementation of devices within a physical network.

Since the definition of what software is considered a medical device in its own right varies significantly between countries, this Technical Report provides guidance on best practices in assuring the safer development, implementation and operation of health software, irrespective of whether it is regulated as a medical device. This Technical Report examines standards that can provide useful guidance for purchasers, implementers and users, as well as for developers and manufacturers through to configuration, implementation, and ongoing use in all care settings and environments. The analysis and guidance provided in this Technical Report recognize that health software is increasingly implemented and operated within a complex 'ecosystem' or 'sociotechnical system' environment where the software is tightly integrated with other systems, technologies, infrastructure, and domains (people, organizations and external environments) and where it also needs to be configured to support local clinical and business processes.

Hence the patient safety benefits and risks associated with implementing individual software components need to be evaluated and managed within the implementing organization's infostructure context, using standards and proven processes that guide and engage both health informatics professionals and clinicians at all stages; a family of standards that enables safety in health software.

Clause 4 of this Technical Report discusses the issues involved with enabling safety, and provides a conceptual framework for standards assessment along with a brief description of the relevant standards.

© ISO 2013 – All rights reserved

Clause 5 builds on this foundational framework by providing an analytical perspective for assessing which standards are most relevant for the various stages of the software lifecycle. This clause also identifies where gaps exist and provides practical guidance on standards based best practices. It is important to note that while the standards discussed in this Technical Report may be useful for enabling safety in health software, in many cases they were not written with that specific purpose in mind.

Who should read this Technical Report?

A common question pervades the discussion on health software safety across this Technical Report: "which standards should be used to enable safety in health software?" This Technical Report is intended for national member bodies and readers who seek an answer to this question.

© ISO 2013 – All rights reserved

Health informatics — Guidance on standards for enabling safety in health software

1 Scope

This Technical Report provides guidance to National Member Bodies (NMBs) and readers by identifying a coherent set of international standards relevant to the development, implementation and use of safer health software. The framework presented in this Technical Report, together with the mapping of standards to the framework, illustrate relevant standards and how they can optimally be applied. The mapping works to clearly demonstrate where standards gaps and overlaps exist. Specifically, this Technical Report:

— identifies a coherent set of international standards that promote the patient-safe (or safer) development, implementation and use of health software,

— provides guidance on the applicability of these standards towards enabling optimal safety in health software within overall risk management and quality management approaches, as well as within the lifecycle steps and processes of health software development,

— addresses the health software safety issues that remain, either as gaps or overlaps between or among the identified standards, and

— discusses how those gaps and overlaps could be addressed—in the short or long term—through revision of the current standards or the development of new ones.

Harm to the operators of health software, should any such risk exist, is outside the scope of this Technical Report.

While there are references in this Technical Report relating to the regulation of health software, it is neither the purpose nor the intention of this Technical Report to prescribe, enforce or endorse regulation; this is recognized as primarily a national or jurisdictional responsibility and is outside the scope of the Technical Report. This Technical Report does, however, attempt to establish an international standards framework that will be globally recognized and accepted, as well as to provide guidance by which jurisdictional authorities within NMBs can choose to propose the implementation of the framework in a regulatory context, if this is desired. Therefore, while it might be beneficial to encourage NMBs to work towards harmonization in regulatory environments, it is not the purpose or intention in any way of this Technical Report to be so prescriptive.

Furthermore, where a standard is recommended for use in this Technical Report, it is not intended to imply that full compliance with all requirements of any recommended standard should be implemented. Compliance is therefore also outside the scope of this Technical Report.

2 Terms and definitions

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

2.1
framework
essential supporting or underlying structure

[SOURCE: ISO 9001:2008]

© ISO 2013 – All rights reserved