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 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

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*.

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

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.

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.

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]

2.2
granularity
level of complexity or the extent to which a system is broken down into smaller parts

Note 1 to entry: While a definition for granularity can be found in ISO 17115:2007, *Health informatics — Vocabulary for terminological systems*, it was not considered applicable to the scope and context of this Technical Report.

2.3
harm
death, physical injury and/or damage to health or wellbeing of a patient

[SOURCE: ISO/IEC Guide 51:1999 modified]

2.4
hazard
potential source of harm

[SOURCE: ISO/IEC Guide 51:1999]

2.5
health informatics
intersection of clinical, IM/IT (Information Management/Information Technology) and management practices to achieve better health

Note 1 to entry: Health informatics involves the application of information technology to facilitate the creation and use of health related data, information and knowledge. Health informatics enables and supports all aspects of health services. [ISO/TC215 Organization Task Force Report (draft) - adapted from www.coachorg.com].

2.6
health software
software used in the health sector that can have an impact on the health and healthcare of a subject of care

Note 1 to entry: This includes:

— software in its basic form that includes systems, items and units (see IEC 62304:2006),

— associated coding systems, inference engines, archetypes and ontologies,

— associated documents needed for implementation, use and service of the software,

— software that is employed, benefits or applies to any part of the health sector, including all public and private organizations or enterprises as well as consumers, and

— software that is commercially and non-commercially available.

2.7
lifecycle
evolution of a system, product, service, project or other human-made entity from conception through retirement

Note 1 to entry: A previous version (1998) of ISO/IEC 12207 defined the software lifecycle model as a “conceptual framework used to organize and manage software product development, operation, maintenance, and retirement activities.” The 1998 edition further noted that “lifecycle models are used to control the evolution of software products from the beginning of their life to their ultimate termination.”

[SOURCE: ISO/IEC 12207:2008]

2.8
medical device
any instrument, apparatus, implement, machine, appliance, implant, *in vitro* reagent or calibrator, software, material or other similar or related article: a) intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the specific purpose(s) of:

— diagnosis, prevention, monitoring, treatment or alleviation of disease,

— diagnosis, monitoring, treatment, alleviation of or compensation for an injury,

— investigation, replacement, modification, or support of the anatomy or of a physiological process,

— supporting or sustaining life,

— control of conception,

— disinfection of medical devices,

— providing information for medical or diagnostic purposes by means of *in vitro* examination of specimens derived from the human body; and

b) which does not achieve its primary intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its intended function by such means

Note 1 to entry: The definition of a device for *in vitro* examination includes, for example, reagents, calibrators, sample collection and storage devices, control materials, and related instruments or apparatus. The information provided by such an *in vitro* diagnostic device may be for diagnostic, monitoring or compatibility purposes. In some jurisdictions, some *in vitro* diagnostic devices, including reagents and the like, may be covered by separate regulations.

Note 2 to entry: Products which may be considered to be medical devices in some jurisdictions but for which there is not yet a harmonized approach, are:

— aids for disabled/handicapped people,

— devices for the treatment/diagnosis of diseases and injuries in animals,

— accessories for medical devices (see Note 3 to entry below),

— disinfection substances, and

— devices incorporating animal and human tissues which may meet the requirements of the above definition but are subject to different controls.

Note 3 to entry: Accessories intended specifically by manufacturers to be used together with a ‘parent’ medical device to enable the latter to achieve its intended purpose should be subject to the same GHTF procedures as apply to the medical device itself. For example, an accessory for a medical device will be classified as though it is a medical device in its own right. This may result in the accessory having a different classification than the ‘parent’ device.

Note 4 to entry: Components to medical devices are generally controlled through the manufacturer’s quality management system and the conformity assessment procedures for the device. In some jurisdictions, components are included in the definition of a ‘medical device’.

[SOURCE: Global Harmonization Task Force (GHTF) Study Group 1: 2005]

2.9
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO 14971:2007]

2.10
risk applicability
relationship, relevancy and appropriateness of risk in a particular context

2.11
risk management
systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating and controlling risk

[SOURCE: ISO 14971:2007]

2.12
risk sharing
form of risk treatment involving the agreed distribution of risk with other parties

Note 1 to entry: Legal or regulatory requirements can limit, prohibit or mandate risk sharing.

Note 2 to entry: Risk sharing can be carried out through insurance or other forms of contract.

Note 3 to entry: The extent to which risk is distributed can depend on the reliability and clarity of the sharing arrangements.

Note 4 to entry: Risk transfer is a form of risk sharing.

[SOURCE: ISO Guide 73:2009]

2.13
risk treatment
process to modify risk

Note 1 to entry: Risk treatment can involve:

— avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk,

— taking or increasing risk in order to pursue an opportunity,

— removing the risk source,

— changing the likelihood,

— changing the consequences,

— sharing the risk with another party or parties (including contracts and risk financing), and

— retaining the risk by informed decision.

Note 2 to entry: Risk treatments that deal with negative consequences are sometimes referred to as 'risk mitigation', 'risk elimination', 'risk prevention' and 'risk reduction'.

Note 3 to entry: Risk treatment can create new risks or modify existing risks.

[SOURCE: ISO Guide 73:2009]

2.14
safety
freedom from unacceptable risk

Note 1 to entry: Health software's role in contributing to iatrogenic harm to patients can be direct (i.e. the design does not meet intended use requirements) or indirect (i.e. the design meets intended use requirements but the system was not configured properly). In the context of patient safety, this involves the reduction of risk of harm associated with health software to an acceptable minimum. This definitional context is under active consideration by the World Health Organization.

[SOURCE: ISO/IEC Guide 51:1999]

2.15
standard
document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context

Note 1 to entry: ISO's international standards are agreements. ISO refers to them as agreements because its members must agree on content and give formal approval before they are published. ISO international standards are developed by technical committees. Members of these committees come from many countries. Therefore, ISO international standards tend to have very broad support.

Note 2 to entry: Standards should be based on the consolidated results of science, technology and experience, and aimed at the promotion of optimum community benefits.

[SOURCE: ISO/IEC Guide 2:2004]

2.16
subject of care
person seeking to receive, receiving, or having received healthcare

Note 1 to entry: Subject of care includes a healthy individual.

[SOURCE: ISO 18308:2011]

3 Abbreviated terms

CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
COCIR	EU Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry
CPOE	Computerized Physician Order Entry
DICOM	Digital Imaging and Communications in Medicine
EHR	Electronic Health Record
EMR	Electronic Medical Record
FDA	Food and Drug Administration
GCM	Generic Component Model
GHTF	Global Harmonization Task Force
HI	Health Informatics
ICT	Information & Communications Technology
ISMS	Information Security Management Systems
ITIL	Information Technology Infrastructure Library
LIS	Laboratory Information System
NHS	National Health Service
NMB	National Member Body
PACS	Picture Archiving and Communication System
QMS	Quality Management system
SDLC	Software Development Life Cycle
SDO	Standards Development Organization
SKMT	Standards Knowledge Management Tool
UCD	User-Centered Design
WHO	World Health Organization

4 Health software safety

4.1 Health software safety incidents

The National Health Service (NHS) *Connecting for Health* IT program established a proactive safety incident management process to address software safety in England. 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. An action plan to address these incidents was initiated with the objective of an incident being made safe within 24 h. Other countries either have no specific data or are in the early stages of collecting and validating data on health software safety incidents or do have some research based studies.[4][5] The NHS data serves as an indication of the

potential for harm to patients as well as the unintended consequences for patient safety posed by health software. Both would likely be much higher had the NHS not established a comprehensive and proactive program to manage software safety risks.

Examples of safety related incidents, from the UK and elsewhere, include the following:

— systems either failing to produce appropriate alerts for patients or not maintaining and updating these alerts to reflect new treatment protocols,

— drug name mapping errors and other errors related to clinical terminology, especially where data are integrated from different care settings, information systems, or organizations,

— wrongly computed ages for patients, e.g. for pre-natal screening or immunization,

— radiotherapy or drug dose rates that were calculated, presented or communicated incorrectly due to calculation or unit conversion errors,

— clinicians incorrectly interpreting clinical data presented to them through an interface from another system without the full context of the presented data also being provided,

— annotations to a medical image not being displayed in the correct position,

— data missing from patient profiles without clinicians being aware of it, due to source systems or interfaces not being available or maintained correctly,

— images from Picture Archiving and Communication Systems (PACS) not being retrievable by clinicians in a timely manner,

— data migration errors when new systems are put into operation or major systems are upgraded,

— software maintenance errors affecting patient identification, that subsequently cause lab or diagnostic results to go to the wrong clinicians,

— clinical decision support rules not being triggered consistently because some of the source data was recorded in a different context or mapped incorrectly,

— security breaches that compromised system integrity or availability, and

— extended unavailability of system operations.

Since patient safety incidents involving health software, as a primary or contributing factor, are often not reported in any systematic way, the development of best practices, reporting systems and an enhanced health software safety culture is as important in health informatics today, as it was in fostering patient safety in clinical practices from as early as the year 2000. Given the increasing complexity of health software arising from component-based approaches, service oriented architectures, inter-organizational systems integration, complex terminologies, and higher degrees of local configurability and decision support algorithms, the benefits as well as the attendant risks will likely both continue to increase. The need for clear guidance and a coherent set of standards is therefore critical for healthcare organizations, vendors and other stakeholders to act in concert to ensure safe, sustainable software implementations and to nurture and foster a strong health software safety culture.

4.2 Health software definitions

Definitions of software, particularly software items, software systems and software units, have been provided through multiple standards including ISO/IEC 90003:2004, *Software Engineering: Guidelines for the application of ISO 9001:2000 to computer software* and IEC 62304:2006, *Medical device software - Software life cycle processes*. Those generic definitions are helpful particularly when addressing granularity, however, there is an ongoing dichotomy drawn when applying software definitions to