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

healthcare. This dichotomy distinguishes between software that is, by definition, a medical device and health software that is not a medical device:

— The former is expressed in the following definition of *medical device software*: "software system that has been developed for the purpose of being incorporated into the medical device or that is intended for use as a medical device in its own right" (see IEC 80001-1:2010 as modified from IEC 62304:2006, 3.12), and

— The latter is expressed in the definition of a *health software product:* "software proffered for use in the health sector for health-related purposes, but excluding software necessary for the proper application of a medical device" (see ISO/TS 25238:2007, 2.3).

As seen from the application of medical device regulations globally, the definition of software as a medical device may vary in certain regulations and may change over time.

The approach of this Technical Report is to utilize a definition of software used in healthcare that encompasses any software that impacts patient care, regardless of whether or not it is deemed medical device software. As noted by the European Union's Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry (COCIR) on medical software subjects in the context of international standardization, COCIR strongly requests that committees, e.g. IEC/TC 62 and ISO/TC 215, develop their standards and other publications with as broad a scope as possible.

This Technical Report targets *health software* with the following characteristics:

— software in its basic form that includes systems, items and units (see IEC 62304:2006). This includes associated digitally stored data such as data tables or rule-sets, coding systems, content models, inference engines, archetypes, ontologies and associated documents needed for use and service of the software,

— software that is used in the health sector, i.e. software that in any part of its lifecycle is consumed, employed, benefits or applied to any part of the health sector. While the words "intended for use" can also be applicable, used is considered the broadest application. Health sector includes all public and private organizations or enterprises that provide for the health and healthcare of individuals, including consumer health services (personal health records, smartphone/tablet applications, etc.), and

— software includes that which is commercially and non-commercially available.

Illustrative examples of health software are:

— patient registries and enterprise master patient indices, electronic health records (EHRs) and electronic medical records (EMRs),

— laboratory information systems,

— drug information systems,

— radiology information systems,

— hospital information systems,

— order entry and results reporting systems,

— immunization reporting and tracking systems,

— scheduling systems for patients, clinicians, or clinical resources (e.g. for surgeries),

— community care systems,

— home care systems,

— personal health records,

— mental health systems or disease specific systems, and

— population health systems insofar as these focus on individuals (e.g. immunizations, alerts, outbreaks, etc.).

It is important to note that as the e-health environment is increasingly integrated, the definition of health software adopted by this report includes patient administrative systems such as appointment scheduling and resources management.

Illustrative examples of software that are not included as health software by way of this Technical Report are:

— financial, human resource, materials management systems,

— population survey and population surveillance systems,

— generic word processing, spreadsheet, or database software systems, and

— telecommunications or networking systems.

4.3 Towards safer health software

The family of standards identified and assessed in this Technical Report provides the means to reduce risk and strive towards safer health software as these standards are adopted.

Software that is safe for all patient interactions, while a worthy goal and desirable end state, is never guaranteed given the impossibility of eliminating all risks. Therefore, an approach based on risk management is followed to reduce all risks involved with health software to acceptable levels. The emphasis in a risk-based approach therefore is about reducing—not necessarily eliminating—risk across the full lifecycle of health software. This applies to the full lifecycle of health software as described in 4.4 and promotes the development, implementation and operation of safer health software.

4.4 Health software lifecycle

A framework for assessing the applicability and utility of standards in enabling safety in health software is needed to determine applicability and also to identify gaps among the standards currently available.

Generally, software lifecycle models are conceptual frameworks used to organize and manage software product development, operation, maintenance, and retirement activities from the beginning of the software life to the ultimate termination of the software (see ISO/IEC 12207:2008). Such lifecycle models provide a means to undertake a comprehensive, complete view and assessment of standards enabling safer health software.

A pragmatic approach to lifecycle models has been taken in this Technical Report to enable such a view and assessment. The following questions are considered fundamental in defining software life cycle steps:

— whether there is a change in risk from one step to another,

— whether there is a different risk profile, risk management characteristic or need for mitigation between one step and another, and

— whether there is a propagation of risk from one step to another.

Any of the above three points being true may imply the need for different standards to be used, thus the need to consider the above questions in the risk analysis.

The lifecycle steps used in this Technical Report are either based on at least one or more standards that already define such steps, or have not been identified in a known standard but do encompass a change in risk or a different risk management profile, characteristic or need, thus implying the need to use a different standard or a gap in the current standards being used.

The process of determining the lifecycle steps is iterative, using the analysis results from a "working software life cycle" to develop a final usable software lifecycle. Overall, what is most useful and straightforward is to understand the minimum number of lifecycle steps that still allow for the robust assessment of standards enabling safety in health software.

It is important to note that a software lifecycle is not the same as a software development lifecycle (SDLC), although software development lifecycle standards do inform this Technical Report. These software lifecycle steps do not presume any particular SDLC.

Also noteworthy for the purposes of this Technical Report, the software lifecycle has both steps and events:

— **steps** are those components of the software lifecycle with associated work activities, assigned resources and outputs, and

— **events** are those components that are significant occurrences at a given place and time.

Health software lifecycle steps include a complex array of linear and iterative actions that together compose the continuous management of that software by all parties involved:

— **developers** are responsible for the design, development, manufacture and maintenance of the health software (also referred to as "manufacturer" or "supplier" in some standards),

— **implementers** are responsible for the installation and integration of the software in a clinical setting (an implementer may be the developer or the owner),

— **owners** are the healthcare organizations procuring the software (and/or may be the implementers for a managed service),

— **operators** are responsible for the provision of the clinical service through the use of health software, and

— **users** are the persons using the health software in the clinical setting, which may include, for example, consumers in the case of personal health records.

Based on the above approach and the information from Annex B, for the purposes of assessing standards for enabling safety in health software, the following lifecycle steps provide germane differentiation of risk profile, characteristics, needs and assumptions.

NOTE 1 These steps do not necessarily imply a linear ordering or time sequence.

NOTE 2 Where available, lifecycle step descriptions are referenced; where not available, lifecycle step descriptions are informative only.

Table 1 — Standards lifecycle descriptions

Standard Lifecycle Step	Substep(s) [a]	Definition	Party(s) [b]
Concept	Document	Conceiving, imagining and specifying the initial design of the aesthetics and primary functions of the software.	D, U
Requirements	Document	A requirement is a need, expectation, or obligation. It can be stated or implied by an organization, its customers, or other interested parties. [see ISO 9000:2005]	D
Design	Document	The phase of software development following analysis, and concerned with how the problem is to be resolved. [see SKMT – Canada Health Infoway Glossary: 2012]	D

Table 1 *(continued)*

Standard Life-cycle Step	Substep(s) [a]	Definition	Party(s) [b]
Development	Code, Test, Document [c]	Design and development is a process (or a set of processes) using resources to transform requirements (inputs) into characteristics or specifications (outputs) for products, processes and systems. [d]	D
Production		Making available the product for client or user.	D
Release	Distribution	A release is a specific version of a configuration item that is made available or released for a particular purpose. [e] [see ISO/IEC 90003:2004]	D, I
Procurement		Purchasing a commercially available product or engaging an organization for the production of "bespoke or in-house developed" software.	D, I, OO
Implementation	Installation Configuration, Integration, Deployment	Software conformance testing and certification may also be included in the implementation step, either as a first or pre-installation step.	D, I, OO
Go-Live		To make some system, which had been under development or operating in a limited test mode, fully active so that its intended users can access it. [see Internet AllWords.com]	I, U, OO
Operation		Any use of the health software within any non-test setting. It is recognized that for new software there may be a lag between it entering operation and full clinical use.	U, OO
Clinical Use		The practical and full use of the software in a clinical setting As linked to this Technical Report's definition of health software, the software step of clinical use and its "... impact on the health and healthcare of a subject of care."	U, OO
Maintenance		Software maintenance in software engineering is the modification of a software product after delivery to correct faults, to improve performance or other attributes. [see ISO/IEC 14764:2006]	D, I, U, OO
Decommission		The system is removed from the operational environments, and system work products and data are archived in the appropriate manner. [f]	D, U, OO
Disposal		Retiring and ending the existence of a system's existing software products or services while preserving the integrity of organizational operations [adapted from ISO/IEC 12207:2008]	D, U, OO

[a] Not every Standard Lifecycle Step has a Substep.

[b] Developer "D" / Implementer "I"/ Owner-Operator "OO" / User "U"

[c] Also known as manufacturer.

[d] Design and development may be treated as different stages of a single integrated design and development process, or as two (or more) separate processes (see ISO 9000, ISO 9001 or ISO 9004).

[e] For this step the system and all associated products are transferred to the client or user.

[f] Data may also be moved or migrated from one system to another, while maintaining semantic integrity.

It is acknowledged by the authors of this Technical Report that the 'language' of the software lifecycle, particularly as it pertains to enabling safety in health software, is not fixed. It is acknowledged that the wording and definitions (where not available in any ISO or other acknowledged standard) may be further refined in future standards development. It is also acknowledged that other software models are available, such as the Generic Component Model (GCM) and its associated taxonomy of standards.[6] A future or further analysis and representation of groups of health software safety applicable standards, such as those summarized in this Technical Report, could be undertaken in subsequent standards developments, using the GCM taxonomy.

A summarization of the lifecycle into the following five categorizations of the lifecycle steps is useful for purposes of this Technical Report:

1) **design:** encompassing concept, requirements and design steps

2) **development:** encompassing development, production and release steps

3) **implementation:** encompassing installation, configuration, integration and go-live steps

4) **operations:** encompassing operation, clinical use and maintenance steps

5) **decommissioning:** encompassing decommissioning and disposal steps

However, from an assessment point of view the above lifecycle steps, at both the detailed level and at the summarized level, are an acceptable software lifecycle framework for undertaking the assessment of health software safety based upon the list of standards.

4.5 How standards were selected for assessment

There are many standards that may be useful to health software developers, implementers and users in enabling safety in health software. In support of this Technical Report and the guidance herein, the identification of standards for assessment has been collated from a variety of sources within a focused set of criteria.

The sources include:

— the published standards and current work program of ISO/TC 215 *Health informatics*,

— the published standards and current work program of ISO/TC 210 *Quality management and corresponding general aspects for medical devices,*

— the published standards and current work program of IEC/TC 62 SC62A *Common aspects of electrical equipment used in medical practice*,

— the published standards and current work program of ISO/TC 176 *Quality management and quality assurance,*

— the published standards and current work program of ISO/IEC JTC 1 and its subcommittees and the work of ISO/IEC Technical Advisory Group, Safety, and

— expert reviews of general, IT market and health informatics standards relating to good development practice and product safety.

Several criteria were applied to determine whether a standard should be among those considered by this Technical Report. A standard was considered if:

— the standard was developed by an international or multinational standards development organization,

— the standard could be used during one or more steps of the health software lifecycle,

— the standard was used in more than one country (as identified in informal review of standards sources as listed above),

— the standard is applicable to, or references, software or health software as identified or defined within this Technical Report, and

— the standard addresses risk and safety.

NOTE All generally applicable standards such as quality standards, risk standards or systems and systems engineering (e.g. JTC 1) standards are noted as applicable foundations of good practice to software life cycle steps, risk management and greater safety and as such are grouped for ease of reference.

There are several other standards that are applicable to the successful design, development, implementation and operation of health software, e.g. attribute standards, i.e. those that identify (and provide related information to) the software characteristics or features necessary, that are testable, and are useful to health software developers, implementers and users in enabling safety in health software. In particular, functional and data standards, applied as necessary throughout the lifecycle of health software, are also foundational to safer health software. The failure to use applicable, purpose-specific attribute standards can constitute a risk at any lifecycle stage of health software.

Several standards that apply to safe health software have accompanying informative guidance for the application of those respective standards. Where relevant safe health software standards have such guidance, that information is noted in the "relationship" details for each specific assessed standard (see Clause 5.1).

4.6 Standards assessed in this Technical Report

Tables 2 and 3 below provide a list of the standards assessed in this Technical Report. The tables include the standard's number, title and the responsible standards development organization (including the Technical / Subcommittee identification). Table 2 lists foundational standards series for health software safety (a series of standards that are overarching in application). Table 3 lists those standards that have a context for either a medical device, or a specific health software.

Table 2 — Foundational standards relevant to safe health software

Scope	Standard(s), Guides and Reports	SDO
Quality Management	ISO 9000:2005 *Quality management systems — Fundamental and vocabulary* ISO 9001:2008 *Quality management systems —Requirements* ISO 10005:2005 *Quality management systems — Guidelines for quality plans* ISO 10006:2003 *Quality management systems — Guidelines for quality management in projects* ISO 10007:2003 *Quality management systems — Guidelines for configuration management* ISO/IEC 90003:2004 *Software engineering — Guidelines for the application of ISO 9001:2000 to computer software* [a]	ISO/TC 176 and ISO/IEC JTC 1 SC 7
[a] ISO/IEC TR 90003, currently under development within ISO/IEC JTC 1/SC 7, is intended to replace ISO/IEC 90003:2004		

Table 2 *(continued)*

Scope	Standard(s), Guides and Reports	SDO
Software and Systems Engineering	ISO/IEC 12207:2008 *Systems and software engineering — Software life cycle processes* ISO/IEC 20000 *Information technology — Service management* (multi-part series) ISO/IEC 25000 *Software Engineering — Software product Quality Requirements and Evaluation (SQuaRE) – Guide to SquaRE* (part of a multi-part series) ISO/IEC 15026 *Systems and software engineering — Systems and software assurance* (multi-part series) ISO/IEC 15504 *Information technology — Process assessment* (multi-part series) Also the ISO/IEC 27000 series known as 'ISMS Family of Standards'	ISO/IEC JTC 1 SC 7 and SC27
Risk Management	ISO 31000:2009 *Risk management — Principles and guidelines* ISO Guide 73:2009 *Risk management — Vocabulary*	ISO Technical Management Board (TMB)
Ergonomics of human-system interaction	ISO 9241-129:2010 *Ergonomics of human-system interaction — Part 129: Guidance on software individualization* ISO/TR 16982:2002 *Ergonomics of human-system interaction — Usability methods supporting human-centred design*	ISO/TC 159
Safety	ISO/IEC Guide 51:1999 *Safety aspects — Guidelines for their inclusion in standards*	Joint ISO/IEC Technical Advisory Group, Safety

[a] ISO/IEC TR 90003, currently under development within ISO/IEC JTC 1/SC 7, is intended to replace ISO/IEC 90003:2004

Table 3 — Standards for a medical device or specific health software context

Standard	Title	SDO
Quality Management	ISO 13485:2003 *Medical devices — Quality management systems — Requirements for regulatory purposes*	ISO/TC 210
Software Life Cycle Processes	IEC 62304:2006 Medical device software — Software life cycle processes	IEC/TC 62 SC62A ISO/TC 210
Risk Management	ISO 14971:2007 *Medical devices — Application of risk management to medical devices*	ISO/TC 210
Risk Management	IEC 80001–1:2010 *Application of risk management for IT-networks incorporating medical devices — Part 1: Roles, responsibilities and activities*	IEC/TC 62 SC62A ISO/TC 215
Security Management	ISO 27799:2008 *Health informatics — Information security management in health using* ISO/IEC 27002 [a]	ISO/TC 215
Safety	ISO/TR 27809:2007 *Health informatics — Measures for ensuring patient safety of health software*	ISO/TC 215
Safety	ISO/TS 25238:2007 *Health informatics — Classification of safety risks from health software*	ISO/TC 215
Usability Engineering	IEC 62366:2007 *Medical devices — Application of usability engineering to medical devices*	ISO/TC 210

[a] Includes references to ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 27005

4.7 Risk management basis

The principal basis for the assessment of standards enabling safety in health software is whether or not the standards address the reduction of risk across lifecycle steps or parts of the software.

Risk management is the systematic application of management policies, procedures and practices to the tasks of analysing, evaluating and controlling risk. In ISO 31000, risk management is defined as "coordinated activities to direct and control an organization with regard to risk. Risk management generally includes risk assessment, risk treatment, risk acceptance and risk communication".

A generic approach to risk management is defined in the widely recognized ISO 31000 and related standards:

— ISO 31000:2009, *Principles and guidelines on implementation*,

— IEC 31010:2009, *Risk management — Risk assessment techniques*, and

— ISO Guide 73:2009, *Risk management — Vocabulary*

ISO 31000 is a starting point for risk management standards development and guidance throughout the life of an organization for a wide range of activities. It can be applied to any type of risk, whatever its nature, whether having positive or negative consequences. It does not deal specifically with safety. Guidance on the introduction of safety aspects into standards is provided in ISO/IEC Guide 51.

Health related risk management is embodied in the medical device standard, ISO 14971:2007, *Medical devices — Application of risk management to medical devices* and its companion IEC/TR 80002-1, *Guidance on the application of* ISO 14971 *to medical device software*. ISO 14971 and IEC/TR 80002-1 are directed to manufacturers of medical devices and medical device software including Laboratory Information Systems (LIS), and Picture Archiving and Communication Systems (PACS).

Health related risk management is also embodied in IEC 80001-1:2010, *Application of risk management for IT-networks incorporating medical devices — Part 1: Roles, responsibilities and activities*, which addresses risk during system implementation and operation.

There is additional useful material on risk management, particularly as it pertains to health software, to be found in ISO/TR 27809:2007, *Health informatics — Measures for ensuring patient safety of health software* and ISO/TS 25238 — *Classification of safety risks from health software*.

Another aspect of risk management as a foundation for enabling safety in health software is the need to address risk sharing and residual risk on health software as it proceeds through its lifecycle. ISO Guide 73 defines risk sharing as "form of risk treatment involving the agreed distribution of risk with other parties."

When a health software product is released (i.e. the release event) to market by a software manufacturer some level of risk to patients remains which is the residual risk.

NOTE From a regulatory standpoint, release of a health software product is also the point at which post-market versus pre-market regulatory and related stipulations may be applied.

The parties responsible for residual and shared risk change throughout the life cycle of the software. For example, when an implementer purchases a commercially available product or engages the production of in-house developed software, the implementer implicitly (and sometimes explicitly) accepts some responsibility for known residual risks. The residual risk notwithstanding, at this point, through whatever means of procurement, the implementer is accepting that the manufacturer's health software meets (or will meet) stated requirements.

When the purchased or in-house developed health software is implemented, new risks (e.g. relating to the configuration, integration, data quality and clinical use of the system) are introduced. Responsibility for managing the full scope of safety risks is then potentially shared among all multiple parties, each with specific responsibilities and inter-dependencies, including the developer, the implementer, to the owner/operator, the health care delivery organization and ultimately, to the users of the system.

At each transition from one lifecycle step to another, and with the involvement of new parties, communication of these risks is essential; for example, respective responsibilities for risk controls and response mechanisms must be clearly defined. Organizations downstream in the software lifecycle need to be aware of these liabilities and the associated risks, as well as the measures they can take to effectively manage those liabilities and risks.

In considering health software, risk sharing is important when looking at standards in order to understand if a standard applies across transition points where risks become shared by multiple parties and if so, which parties involved (developer, implementer, owner-operator and/or user) must take action to manage risk.

4.8 Human factors basis

The discipline of human factors is the study of how people interact physically and psychologically with products, tools, procedures, and processes. Its principal aim is to adapt technology to function in a way that seems natural to people.

The complexity of healthcare systems has increased dramatically in the last few years. As a result, healthcare professionals must now interact with many systems that are often not designed to take into account human capabilities. When dealing with such complex systems, errors are likely to occur. Integrating a human factors approach in the culture of an organization and adopting a User-Centered Design (UCD) approach to designing healthcare systems will work to reduce the likeliness of errors and promote safer health software.

The human factors discipline is an important part of health software development and ensures health software is designed in an iterative matter with the involvement of actual end users. It also establishes organizational processes that are focused on making sure health software is well adapted to humans and their environment.

ISO 9241 is a multi-part standard providing a comprehensive foundation addressing various elements of the ergonomics of human-computer interaction.

The following two complementary standards outline human factors principles to be followed when designing medical devices:

— IEC 62366:2007, *Medical devices — Application of usability engineering to medical devices, which addresses human factors design processes*, and

— ANSI/AAMI HE75.2009, *Human factors engineering — Design of medical devices*, which focuses on human factors design principles.

While these two standards focus on medical devices, the same important principles are applicable to health software and include:

a) **Involving users early and often in the design process** - Involving users from the very beginning of the design process will help promoting a UCD approach. Both standards describe ways in which this can be accomplished.

b) **For designers to consider user characteristics, capabilities, and preferences** - For health software to be efficient and safer, user capabilities and limitations need to be integrated into design. HE75 outlines design principles that should be considered by designers to ensure health software is well-designed and safe to use. Design guidelines related to vision, audition, information processing, memory, response capabilities, and ergonomics should be taken into account for safer health software. Heuristic principles (see ZHANG) can be used to assess whether health software conforms to basic design principles.[7]

c) **Managing the risk of use error** - Methods to help manage the risk of use error are presented in HE75. A use-error risk management process is also outlined. This process is an important part of the human factors framework for safer health software and will benefit from being integrated with risk management frameworks.

d) **Acting on human factor guidelines for design principles, environmental considerations, user documentation, cross-cultural factors, accessibilities, software user interfaces, ergonomics, and home healthcare** - There are many aspects of human factors to be considered to promote safer health software. HE75 outlines several of these and provides guidelines to be followed by designers to ensure systems are well adapted to humans.

e) **Following usability engineering processes and iterative design** - Usability engineering is at the heart of the human factors framework. It promotes an iterative design approach by testing and validating systems against end-users. Feedback obtained through this process is fed back to the design cycle, allowing iterative mitigation of risk and safety related issues.

NOTE Additional references on frameworks and models for human factors, and incorporating usability and improving the user experience in healthcare organizations, are emerging in various writings including Vicente[8] and Staggers.[9]

4.9 Granularity

In the context of standards enabling safety in health software, granularity means the level of complexity or the extent to which a system is broken down into smaller parts. In software development, this means providing a clear definition of how critical parts should behave to a level that permits code to be written from it. This could include everything from an individual software element (such as a systolic blood pressure data value) through to an integrated solution implemented across a jurisdiction.

IEC 62304 provides one approach to software granularity, focusing on the development phase of the software at three levels: system, item and unit. For the purpose of assessing the level of applicability of a standard to safety in health software and taking into account some illustrative examples of health software, this Technical Report uses the following three levels of granularity:

— **Components:** the unit level of health software that includes data, objects or other entities configured and usable within or by a computer program,

NOTE 1 This includes item and unit development (see IEC 62304:2006).

— **Application:** a computer program or series of computer programs that serve an identifiable and specific business purpose. In health software, applications serve an identifiable and specific health business purpose, and

NOTE 2 This includes system development (see IEC 62304:2006).

— **Enterprise Application:** an entity or organization comprising people, processes, information and technology that uses an application or series of applications to support the business of the entire enterprise.

5 Standards assessment and guidance

5.1 Standards assessment

To assess a standard whose use may enable safety in health software, the following questions need to be answered:

a) Is this standard useful for improving patient safety in the development, implementation, or operation of health software (i.e. for reducing risks)?

b) At what level of granularity of health software does the standard apply?

c) At what step(s) of the health software lifecycle does the standard apply?

In answering these questions, the following standards-related information is used:

— the standard's identification number, publication date (or development status if not yet published) and title,

— scope of the standard,

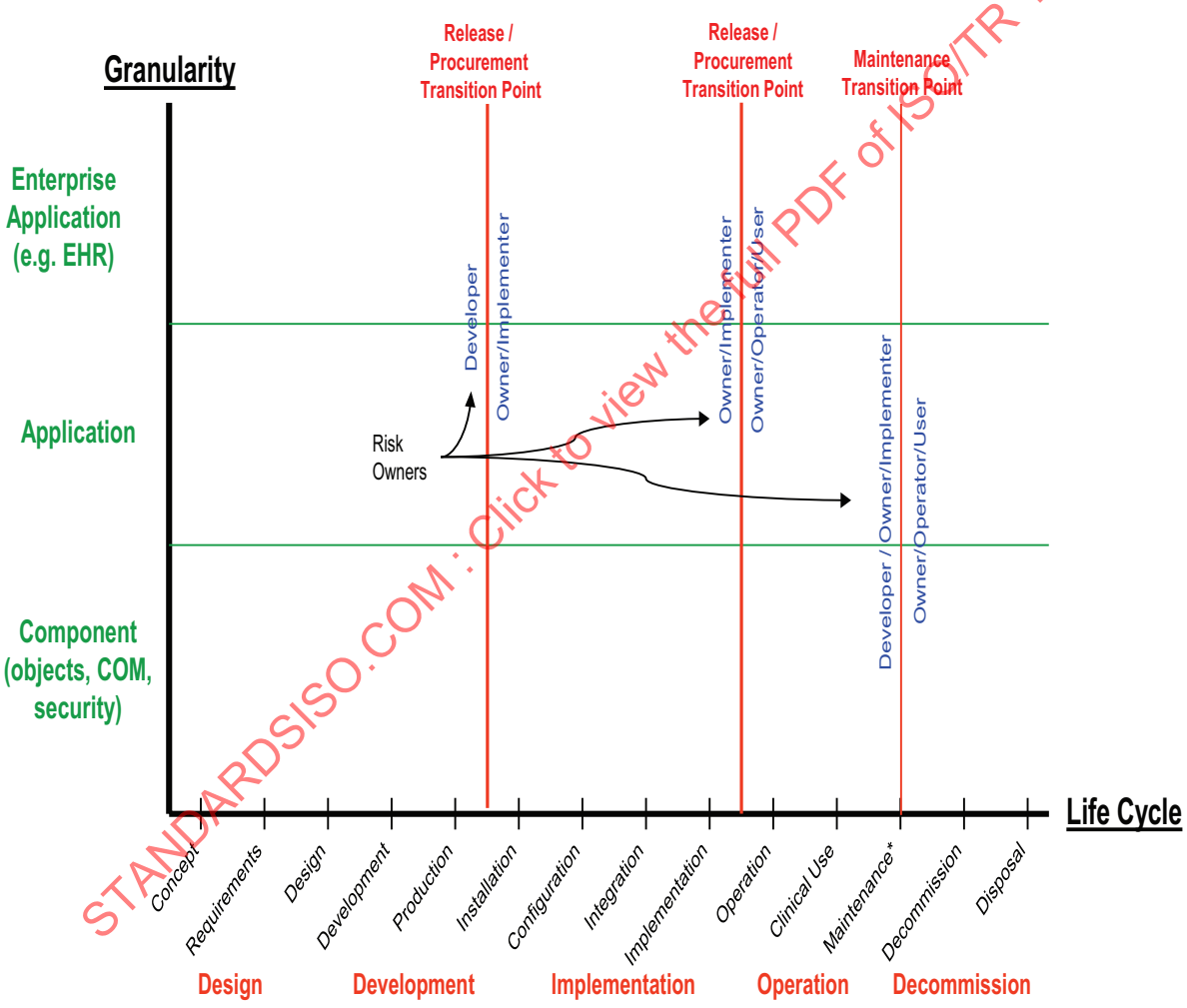
— risk applicability or acceptability (also noting controls),

— evidence of the standard's use (if available),

— software lifecycle coverage and software granularity coverage, and

— the relationship of the standard to other standards.

The framework for assessing and mapping standards is best founded upon a two dimensional matrix or table of granularity and lifecycle steps. Figure 1 shows the elements of the matrix and an identification of transition points where risk becomes shared by multiple parties.



NOTE The health software lifecycle steps, while identified linearly on the figure above, do include a complex array of linear and iterative actions to provide the continuous management of that software by all parties involved. For example, maintenance includes iterative, repeat points of risk sharing.

Figure 1 — Risk shared by multiple parties during the health software life cycle

The first five assessments provide guidance on foundation standards series and are overarching in the scope of application. These standards are the foundation for health software specific standards, and likewise are also the foundation for addressing health software risk and safety. These standards

provide useful best practices for software generally and this includes health software, and as such are part of a coherent view of standards that may be used for the patient-safe development, implementation and use of health software. The five series following are either "organizational" or "ICT domain wide" or "enterprise risk or safety generic" in scope and their use should be taken from those specific perspectives.

The assessment following the foundation series (see Clause 5.1.6 and on) are specific standards that apply to patient-safe development, implementation and use of health software.

5.1.1 Quality management standards

5.1.1.1 Scope

The ISO quality management standards are concerned with quality management systems and are designed to help organizations ensure they meet the needs of their customers. Standards include:

— ISO 9000:2005, *Quality management systems — Fundamentals and vocabulary*,

— ISO 9001:2008, *Quality management systems — Requirements*,

— ISO 10005:2005, *Quality management systems — Guidelines for quality plans*,

— ISO 10006:2003, *Quality management systems – Guidelines for quality management in projects*, and

— ISO 10007:2003, *Quality management systems – Guidelines for configuration management*.

NOTE ISO/IEC TR 90003[1)], *Guidelines for the application of ISO 9001:2000 to computer software* is a cornerstone standard for the application of quality management systems to software life cycle processes. It is currently under development within JTC 1/SC 7 and is intended to replace ISO/IEC 90003:2004,*Software engineering - Guidelines for the application of ISO 9001:2000 to computer software* in early 2013.

5.1.1.2 Risk applicability/acceptability

While this family of standards is not applicable specifically to health software safety, ISO 9001 is the *de facto* standard in creating and maintaining a quality management system. Adherence to the quality processes and practices defined in a organization's quality management system is expected to result in the delivery of products and services which meet the needs of customers and applicable statutory and regulatory requirements.

5.1.1.3 Evidence of use

These standards are widely deployed and used across all industry sectors.

5.1.1.4 Lifecycle and granularity coverage

Not applicable to lifecycle of software or granularity of software.

5.1.1.5 Relationship

ISO 13485:2003 is the medical device industry's equivalent of ISO 9001:2008 and was created from 9001 to allow it to be used for regulatory purposes.

5.1.2 Software and systems engineering standards

5.1.2.1 Scope

ISO/IEC JTC 1 *Information Technology* develops and maintains standards across a broad range of ICT domains, working through 19 fully constituted SCs (each with many respective Working Groups) and

1) To be published.

2 WGs that report directly to JTC 1. JTC 1 and its SCs/WGs are currently responsible for over 2,500 published standards. ISO/IEC JTC 1/SC 7 *Software and systems engineering* is the principal group within JTC 1 relevant to health software safety in the broadest sense.

NOTE The following are links to the JTC 1 home page for the latest information: http://www.iso.org/iso/jtc1_home and http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45020.

5.1.2.2 Risk applicability/acceptability

Software safety has its origins in the appropriate management of the entire software life cycle within a governance and compliance framework that supports software system quality and assurance. The principal standards from JTC 1 that are relevant include the following:

5.1.2.2.1 ISO/IEC 12207 *Systems and software engineering - Software life cycle processes*

The application of this International Standard (and the companion ISO/IEC 15288 on system life cycle processes) is currently elaborated in the three Technical Reports of ISO/IEC 24748 *Systems and software engineering — Life cycle management* with:

— *Part 1: Guide for life cycle management,*

— *Part 2: Guide to the application of* ISO/IEC 15288 *(previously* ISO/IEC TR 19760*),* and

— *Part 3: Guide to the application of* ISO/IEC 12207 *(previously* ISO/IEC TR 15271)

NOTE Part 4 to ISO/IEC 24748 is in preparation and will eventually replace ISO/IEC 26702:2007, *Systems engineering — Application and management of the systems engineering process*, which specifically mentions health and safety factors in a systems engineering context.

5.1.2.2.2 ISO/IEC 15504 Information technology - Process assessment

Software and systems safety is taken a step further in this multi-part standard which includes International Standards, Technical Specifications and Technical Reports, including the following:

— *Part 1: Concepts and vocabulary,*

— *Part 2: Performing an assessment,*

— *Part 3: Guidance on performing an assessment,*

— *Part 4: Guidance on use for process improvement and process capability determination,*

— *Part 5: An exemplar software life cycle process assessment model,*

— *Part 6: An exemplar system life cycle process assessment model,*

— *Part 7: Assessment of organizational maturity,*

— *Part 8: An exemplar process assessment model for IT service management,*

— *Part 9: Target process profiles, and*

— *Part 10: Safety extension*

5.1.2.2.3 ISO/IEC 15026 *Systems and software engineering - Systems and software assurance*

Approaches for assuring the risk and integrity of software products as software engineering artefacts are addressed in ISO/IEC 15026 which originates from IEEE and provides for an assurance case that is targeted for a “safety case”. ISO/IEC 15026 comprises:

— *Part 1: Concepts and vocabulary,*

— *Part 2: Assurance case,*

— *Part 3: System integrity levels,* and

— *Part 4: Assurance in the lifecycle*

5.1.2.2.4 ISO/IEC 20000 *Information technology – Service management*

ISO/IEC 20000 addresses the information technology service management domain and provides an organizational equivalent to the ITIL certification. It includes the following key parts:

— *Part 1: Service management system requirements,*

— *Part 2: Guidance on the application of service management systems,*

— *Part 3: Guidance on scope definition and applicability of* ISO/IEC 20000-1,

— *Part 4: Process reference model,*

— *Part 5: Exemplar implementation plan for* ISO/IEC 20000-1,

— *Part 7: Application of* ISO/IEC 20000-1 *to the cloud* (In progress),

— *Part 10: Concepts and terminology for* ISO/IEC 20000-1 (In progress),

— *Part 11: Guidance on the relationship between* ISO/IEC 20000-1 *and related frameworks.* (In progress)

NOTE ISO/IEC TR 20000-11 gives guidance on the relationship between ISO/IEC 20000-1 and ITIL.

5.1.2.2.5 ISO/IEC 25000 *Software engineering – Software product quality requirements and evaluation*

ISO/IEC 25000:2005 addresses the "SQuaRE" process. Other key standards and specifications that relate to ISO/IEC 25000 include:

— ISO/IEC 25001:2007 *Software engineering – Software product quality requirements and evaluation - Planning and management*,

— ISO/IEC 25010:2011 *Software engineering – Software product quality requirements and evaluation - System and software quality models*,

— ISO/IEC 25012:2008 *Software engineering – Software product quality requirements and evaluation - Data quality model*,

— ISO/IEC 25020:2007 *Software engineering – Software product quality requirements and evaluation - Measurement reference model and guide*,

— ISO/IEC 25021:2012 *Software engineering – Software product quality requirements and evaluation - Quality measure elements*,

— ISO/IEC 25040:2011 *Software engineering – Software product quality requirements and evaluation - Evaluation process (revision of* ISO/IEC 14598-1:2009*)*, and

— ISO/IEC 25045:2010 *Software engineering – Software product quality requirements and evaluation - Evaluation module for recoverability*

ISO/IEC 25010, which replaces ISO/IEC 9126, *Software engineering — Product quality*, assists in the assessment and evaluation of system and software product quality. It has distinct applicability in that it provides a generic methodology for assessment and evaluation of the quality of software but does not translate this into risk assessment. ISO/IEC 25010 can therefore be applied to all software products and is capable of being used to identify risk given some metric or translation of the results defined for this activity. It has applicability to health software safety particularly in the assessment of the 'quality

in use' measures, i.e. effectiveness, efficiency, satisfaction, safety and usability. It provides both broad and specific evaluation parameters. These parameters define a consistent terminology for specifying, measuring and evaluating system and software product quality. ISO/IEC 25010 also provides a set of quality characteristics against which stated quality requirements can be compared for completeness.

5.1.2.3 Evidence of use

These standards are widely deployed and used across all industry sectors.

5.1.2.4 Lifecycle and granularity coverage

These JTC 1/SC 7 standards cover software, primarily as components and applications, with variable applicability to enterprise applications. The lifecycle coverage strongly covers design and development, again with variable coverage on implementation and operations.

5.1.2.5 Relationship

The JTC 1/SC 7 standards reference herein, while not addressing health software specifically, do address software overall in the general ICT domain and associated process, risk and safety requirements.

NOTE See ANNEX C for further scope information on key JTC 1/SC 7 standards identified above.

5.1.3 Risk management standards

5.1.3.1 Scope

ISO 31000:2009, *Risk management — Principles and guidelines* provides a generic approach to managing risks in an enterprise. The standard is not specific to health or any other sector. ISO 31000 addresses risk identification, assessment and treatment, communications and consultations, and monitoring and review.

5.1.3.2 Risk applicability/acceptability

ISO 31000 provides a universally recognized paradigm for practitioners and companies employing risk management processes to replace the myriad of existing standards, methodologies and paradigms that differed between industries, subject matters and regions.

5.1.3.3 Evidence of use

This is a relatively new standard that is now being widely deployed across all industry sectors.

5.1.3.4 Lifecycle and granularity coverage

The standard can be applied to all phases of a system or software lifecycle. It provides guidance at a high level.

5.1.3.5 Relationship

ISO 31000 is related to the following:

— IEC 31010:2009, *Risk management — Risk assessment techniques*, and

— ISO Guide 73:2009, *Risk management — Vocabulary.*

The principles, guidelines and methods described in these standards are a good starting point when risks in addition to patient safety need to be considered (see ISO 31000:2009, 4.7). They are consistent with the risk management techniques and the use of meta-language in identifying physical causes in

ISO 14971:2007 to medical devices and also similarly consistent with IEC/TR 80002-1, *Guidance on the application of* ISO 14971 *to medical device software*.

5.1.4 Ergonomics of human-system interaction standards

5.1.4.1 Scope

The ISO 9241 standards were originally titled *Ergonomic requirements for office work with visual display terminals (VDTs)*. From 2006, the standards were retitled to the more generic *Ergonomics of human-system interaction* and are not specific to health or any other sector. ISO 9241 and related standards are usability standards primarily concerned with product use, user interface and interaction, processes of product development and the application of user centred design.

5.1.4.2 Risk applicability/acceptability

ISO 9241 standards are targeted to designers and developers of hardware and software products and provide a widely recognized basis for human interaction with hardware and software. As a pre-curser to specific human factors engineering in health software and acknowledging that poor usability can increase the risk of inadvertent introduction of hazards, these standards are a useful foundation for human factors engineering in health software.

5.1.4.3 Evidence of use

These standards are widely deployed and used across all industry sectors.

5.1.4.4 Lifecycle and granularity

These standards are primarily applied to the design and development of a system or software lifecycle.

5.1.4.5 Relationship

ISO 9241 is a multipart standard series, as follows:

— 100 series: *Software ergonomics*,

— 200 series: *Human system interaction processes*,

— 300 series: *Displays and display related hardware*,

— 400 series: *Physical input devices - ergonomics principles*,

— 500 series: *Workplace ergonomics*,

— 600 series: *Environment ergonomics*,

— 700 series: *Application domains - Control rooms*, and

— 900 series: *Tactile and haptic interactions*

These standards, including for example, ISO 9241-210:2010, *Ergonomics of human-system interaction — Human-centred design for interactive systems*, provide some of the most pertinent insights on human factors design principles and processes, with the focus on interactive software applications, which distinguishes these standards from other standards focused on medical devices.

While the focus of the ISO 9241 standards is on ‘standalone’ systems with safety more of a by-product than an overt objective, the level of detail and the degree to which principles are translated into practical process suggestions provide a body of knowledge that can be effectively tailored and adapted to the health software ecosystem.

5.1.5 Safety guidance

5.1.5.1 Scope

ISO/IEC Guide 51 provides standards developers with guidelines for the inclusion of safety aspects in standards. ISO/IEC Guide 51 is the generic guide to standards development for safety related standards. It is applicable to any safety aspect related to people, property or the environment, or a combination of one or more of these (e.g. people only; people and property; people, property and the environment).

5.1.5.2 Risk applicability/acceptability

ISO/IEC Guide 51 adopts an approach aimed at reducing the risk arising from the use of products, processes or services. The complete life cycle of a product, process or service, including both the intended use and the reasonably foreseeable misuse, is considered. The Guide focuses on the concept of safety and achieving safety by reducing risk to a tolerable level.

5.1.5.3 Evidence of use

The concepts and definitions of safety and risk are used extensively in medical device related standards including ISO 14971 and others.

It is noted that ISO/IEC Guide 51 is under review and revision and that associated Guides (e.g. ISO/IEC Guide 63:2012, *Guide to the development and inclusion of safety aspects in International Standards for medical devices*) are available that address specific medical device application and context for ISO/IEC Guide 51.

5.1.5.4 Lifecycle and granularity coverage

By its very definition of scope, ISO/IEC Guide 51 can be applied to standards development for all phases of a software lifecycle and levels of granularity. It provides guidance at a context and definition level.

5.1.5.5 Relationship

ISO/IEC Guide 51:1999 is a second edition, revising the first edition published in 1990. ISO/IEC Guide 51 was the first of a series of guides intended to provide a harmonized approach to the concept of safety when preparing International Standards. ISO/IEC Guide 51 anticipated the need for sector guidance such as ISO/IEC Guide 63. Consistent with ISO/IEC Guide 51, additional guidance might be needed for sectors within the broad category of medical devices.

NOTE 1 The scope of ISO/IEC Guide 63 is to provide guidance to standards writers on how to include safety aspects in the development of medical device safety standards intended to be used within the risk management framework established in ISO 14971. It expands on the concepts developed in ISO/IEC Guide 51 to include safety-related performance and usability.

NOTE 2 ISO Guide 73:2009, *Risk management — Vocabulary*, while not a specific safety Guide, provides the definitions of generic terms related to risk management. It aims to encourage a mutual and consistent understanding of, and a coherent approach to, the description of activities relating to the management of risk, and the use of uniform risk management terminology in processes and frameworks dealing with the management of risk.

5.1.6 ISO 13485:2003 *Medical devices – Quality management systems – Requirements for regulatory purposes*

5.1.6.1 Scope

This International Standard specifies requirements for a quality management system where an organization needs to demonstrate its ability to provide medical devices and related services that consistently meet customer requirements and regulatory requirements applicable to medical devices and related services.

5.1.6.2 Risk applicability/acceptability

As the focus is facilitating harmonized medical device regulatory requirements for quality management systems, it is primarily about reducing risk through the consistent application of quality management processes. It is applied by the software manufacturer to the production or design/development and production of their medical device regulated product(s).

5.1.6.3 Evidence of use

ISO 13485 and its variants (e.g. the FDA's Quality System Requirements) are used to regulate applicable medical device software and specifically identified applications and components of health software in the European Union, Canada, and the USA.

5.1.6.4 Lifecycle and granularity

Applies to Design (concept to design) and Development (development and production) including components and applications.

5.1.6.5 Relationship

ISO 13485:2003 is based on ISO 9001:2000 (it has the same format as ISO 9001:2000 and most of the same requirements) but in particular the requirements for "customer satisfaction" and "continual improvement" have been modified.

ISO 13485:2003 has an accompanying guidance standard, ISO/TR 14969:2004, for the application of the requirements for quality management systems. It does not add to, or otherwise change, the requirements of ISO 13485. This Technical Report does not include requirements to be used as the basis of regulatory inspection or certification assessment activities. ISO/TR 14969 is not specific to software, but rather is applicable to all medical devices and provides guidance that can be used to better understand the requirements of ISO 13485 and to illustrate some of the variety of methods and approaches available for meeting the requirements of ISO 13485.

5.1.7 IEC 62304:2006, *Medical device software — Software lifecycle processes*

5.1.7.1 Scope

This standard defines the life cycle requirements for medical device software. The set of processes, activities and tasks described in this standard establishes a common framework for medical device software life cycle processes.

5.1.7.2 Risk applicability/acceptability

IEC 62304 is specific to medical device software, including software that itself is a medical device. The standard specifies the attributes of a quality management system (QMS) that a software manufacturer would apply to its software life cycle including design, development, production and maintenance; these process attributes are sensitive to the risk assessment and analysis that a software manufacturer would undertake – a process for which is also specified in the standard.

5.1.7.3 Evidence of use

IEC 62304 is increasingly being used and referenced by vendor companies in the EU and the USA.

5.1.7.4 Lifecycle and granularity

Applies to Design (concept to design) and Development (development, production and post-production), as well as to components and applications.

5.1.7.5 Relationship

Medical device management standards such as ISO 13485 and ISO 14971 provide a management environment that lays a foundation for an organization to develop products. Safety standards such as IEC 60601-1 and IEC 61010-1 give specific direction for creating safe medical devices. When software is a part of these medical devices, IEC 62304 provides more detailed direction on what is required to develop and maintain safe medical device software. IEC 62304 was derived from ISO/IEC 12207 and contains a cross reference table that relates the two standards.

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

5.1.8.1 Scope

ISO 14971 specifies a process for a manufacturer to identify the hazards associated with medical devices, including *in vitro* diagnostic (IVD) medical devices, to estimate and evaluate the associated risks, to control these risks, and to monitor the effectiveness of the controls.

5.1.8.2 Risk applicability/acceptability

The standard specifies the process a manufacturer uses to identify, quantify, and manage risks. It is referenced by IEC 62304 and is often used by manufacturers as evidence of meeting the risk management elements of ISO 13485.

5.1.8.3 Evidence of use

A number of jurisdictions have legislated that the requirements of ISO 14971 must be met. Some of these (not an exhaustive list) include: South Africa, Argentina, and Brazil.

5.1.8.4 Lifecycle and granularity coverage

ISO 14971 applies to Design (concept to design) and Development (development and production) and for developer use, also to post production lifecycle steps, as well as to components and some applications.

5.1.8.5 Relationship

ISO 14971 provides requirements for the risk management process to IEC 62304 and is amplified by IEC 62304.

ISO 14971 has an accompanying guidance, IEC/TR 80002-1:2009, that provides guidance for the application of the requirements contained in ISO 14971 to medical device software with additional references to IEC 62304:2006, *Medical device software — Software life cycle processes*. IEC/TR 80002-1 does not add to, nor otherwise change, the requirements of ISO 14971:2007 or IEC 62304:2006.

The guidance in IEC/TR 80002-1 is aimed at risk management practitioners who need to perform risk management when software is included in the medical device/system, and also at software engineers who need to understand how to fulfil the requirements for risk management as specified in ISO 14971.

It should be noted that even though ISO 14971 and the accompanying IEC/TR 80002-1 focus on medical devices, IEC/TR 80002-1 may be used to implement a safety risk management process for any health software in the healthcare environment independent of whether the health software is classified as a medical device. IEC/TR 80002-1 provides excellent guidance regarding how health software safety risks may be evaluated and quantified during design and development, including providing useful annexes with examples.

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

5.1.9.1 Scope

IEC 80001-1:2010 defines the roles, responsibilities and activities that are necessary for risk management of IT-networks incorporating medical devices to address the key properties of safety, effectiveness and data and systems security. This standard does not specify acceptable risk levels.

5.1.9.2 Risk applicability/acceptability

This standard is specific to risk management as it applies to inclusion of a medical device(s) into an IT network. This standard is uniquely important in that it applies to the owner/operator or other party as the responsible organization.

In particular, IEC 80001-1:2010 specifies the process which a responsible organization uses to identify, quantify, and manage risks, including the mandatory assignment of roles within the organization: the responsible organization is required to appoint people to certain roles defined in this standard. This standard defines the responsibilities of those roles. The most important of those roles is the medical IT network risk manager. This role can be assigned to someone within the responsible organization or to an external contractor.

For example, the incorporation or removal of a medical device or other components in an IT network is a task which requires design of the action; this might be out of the control of the manufacturer of the medical device.

5.1.9.3 Lifecycle and granularity coverage

IEC 80001-1 applies to Implementation (and Operation, including clinical use) as well as to enterprise applications only.

5.1.9.4 Relationship

Risk management activities in IEC 80001-1 are based largely on those of ISO 14971 but go beyond safety as defined in the latter. The life cycle management activities described in this International Standard are very similar to those of ISO/IEC 20000-2, *Information technology — Service management — Part 2: Guidance on the application of service management systems*. Additional parts of the 80001 series will provide guidance and tools for the application of IEC 80001-1. Four guidance documents have been completed and others are under development, as follows:

— *Part 2-1 Step by step risk management of medical IT-networks; Practical applications and examples* provides a step-by-step guide to applying risk management when creating and altering a medical IT network. It illustrates this with examples and information on the identification and control of the associated risks. It should be noted that it is not a full interpretation of IEC 80001-1:2010, as it only details the steps involved in executing IEC 80001-1 (see Clause 4.4).

— *Part 2-2 Guidance for the disclosure and communication of medical device security needs, risks and controls* provides guidance on how the security capabilities from IEC 80001-1 may be disclosed and discussed between the stakeholders in a medical device IT network project. It provides a framework for this security dialogue to occur.

— *Part 2-3 Guidance for wireless networks* provides practical advice on risk management required for the use of wirelessly enabled and networked medical devices. It does not follow a methodology but discusses each particular wireless feature and potential risk separately, and

— *Part 2-4 General implementation guidance for healthcare delivery organizations* helps the healthcare delivery organization assess the impact of the IEC 80001-1 standard on the organization and establish a series of business as usual processes to manage risk in the creation, maintenance and upkeep of its medical IT networks.

5.1.10 ISO 27799:2008, *Health informatics — Information security management in health using ISO/IEC 27002*

5.1.10.1 Scope

ISO 27799 defines guidelines to support the interpretation and application in healthcare of ISO/IEC 27002 and is a companion to that standard. ISO 27799 specifies a set of detailed controls for managing health information security and provides best practice guidelines and mandatory requirements to protect the confidentiality, integrity and availability of personal health information. These include requirements for design, development, implementation and maintenance of information systems.

5.1.10.2 Risk applicability/acceptability

ISO/IEC 27002 is a code of practice which specifies controls for an information security management system (ISMS). ISO/IEC 27002 is a broad, complex standard and its advice is not tailored specifically to healthcare. ISO 27799 supports the implementation of ISO/IEC 27002, within health environments, in a consistent fashion and with particular attention to the unique challenges that the health sector poses. Controls are declared mandatory where these are considered essential for protecting patient safety. By following ISO 27799, healthcare organizations help to ensure that the confidentiality and integrity of data in their care are maintained, that critical health information systems remain available, and that accountability for health information is upheld.

5.1.10.3 Lifecycle and granularity coverage

Applies to design, development, implementation and operation (i.e clinical use and ongoing maintenance), as well as to enterprise applications and applications.

5.1.10.4 Relationship

Selecting and applying the security controls of ISO/IEC 27002:2013 will be based on assessment of risks in the particular environment. Thus ISO 27799:2008 constrains some of the controls by a general assessment for health information.

ISO 27799 is a healthcare specialization of ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security management*, which provides a list of commonly accepted control objectives and best practice controls to be used as guidance when selecting and implementing controls for achieving information security. ISO/IEC 27002 is part of the ISO/IEC 27000 family of standards.

The core standard of the ISO/IEC 27000 family is ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*, which specifies the requirements for establishing, operating, monitoring, reviewing, maintaining and improving formalized information security management systems within the context of the organization's overall business risks.

ISO/IEC 27005, *Information technology — Security techniques — Information security risk management* provides guidelines for information security risk management, including advice on risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and risk review.

NOTE 1 ISO/IEC 27001 formally defines the mandatory requirements for an Information Security and Management system (ISMS). It uses ISO/IEC 27002 to indicate suitable information security controls within the ISMS. An organization can be audited against ISO/IEC 27002, but there is no way to be "certified" against it because it is a code of practice. An organization can be audited against ISO/IEC 27001 and obtain a certificate of compliance.

NOTE 2 Information security standards have direct applicability to managing safety in the use and operation of health software by providing information integrity and availability safeguards.

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

5.1.11.1 Scope

This Technical Report considers the control measures required to ensure patient safety in respect to health software products. It does not apply to software which is:

— necessary for the proper application of a medical device,

— an accessory to a medical device, or

— a medical device in its own right.

The Technical Report does, however, start with considering software lifecycle controls that are applied to medical devices which offer practical solutions and how these controls can be adapted for health software products.

One notable aim of the Technical Report is to identify what standards may be best used, or created, if health software products were to be regulated or controlled in some manner.

5.1.11.2 Risk applicability/acceptability

A strong focus of the Technical Report is risk management as one of the control measures. In this respect, the document considers a number of available risk management standards (including non-health standards, e.g. IEC 61508) and includes the risk classifications from ISO/TS 25238.

5.1.11.3 Lifecycle and granularity coverage

With 'design controls' being explicitly defined as one of the possible measures, the standard implicitly focuses on the initial lifecycle stages (design and development). The Technical Report, however, recognizes that steps have to be taken to address risks emerging later in the lifecycle. The Technical Report's scope applies predominantly to applications, though it could be considered for components.

5.1.11.4 Relationship

The Technical Report makes reference to a significant number of related standards. ISO/TR 27809 is a source reference to this Technical Report and covers similar scope and issues. It is intended that ISO/TR 17791 provides an updated and current view to the issues of standards to be best used to ensure patient safety in respect to health software.

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

5.1.12.1 Scope

This Technical Specification is concerned with the safety of patients and gives guidance on the analysis and categorization of hazards and risks to patients from health software products, in order to allow any product to be assigned to one of five risk classes. It applies to hazards and risks which could cause harm to a patient. Other risks, such as financial or organizational risks, are outside the scope of this Technical Specification unless they have the potential to harm a patient.

ISO/TS 25238 applies to any health software product, whether or not it is placed on the market and whether it is for sale or free of charge. Examples of the application of the classification scheme are given. This Technical Specification does not apply to any software which is necessary for the proper application or functioning of a medical device.

5.1.12.2 Risk applicability/acceptability

This Technical Specification focuses on a risk classification where the level of risks can be represented in a risk matrix; the classification is structured with likelihood and consequence forming its two dimensions. ISO/TS 25238 is specific to health software and provides a process of risk assignment.

5.1.12.3 Lifecycle and granularity coverage

As the analysis for risk assignment encompasses all those involved from design to development, implementation, use and maintenance, this International Standard focuses on all life cycle stages, except for decommissioning. It also applies to predominantly to applications, though it could also be considered for components of applications.

5.1.12.4 Relationship

ISO/TS 25238 is a 'stand-alone' Technical Specification, but is closely related to ISO/TR 27809.

NOTE ISO/TS 25238 is planned for withdrawal and incorporation into the IEC 80001 standard.

5.1.13 IEC 62366:2007, Medical devices — Applicability of usability engineering to medical devices

5.1.13.1 Scope

This International Standard specifies a process for a manufacturer to analyse, specify, design, verify and validate usability, as it relates to safety of a medical device. This usability engineering process assesses and mitigates risks caused by usability problems associated with correct use and use errors, i.e. normal use. It can be used to identify but does not assess or mitigate risks associated with abnormal use.

NOTE For the purposes of this International Standard, usability is limited to characteristics of the user interface. This standard does not apply to clinical decision making relating to the use of a medical device.

If the usability engineering process detailed in this International Standard has been complied with, and the acceptance criteria documented in the usability validation plan have been met, then the residual risks, as defined in ISO 14971, associated with usability of a medical device are presumed to be acceptable, unless there is objective evidence to the contrary.

5.1.13.2 Risk applicability/acceptability

IEC 62366 describes the usability engineering process at a very high level and is consistent with a risk management approach such as provided by ISO 14971.

The standard is targeted to manufacturers and standards setters, not implementing organizations, so it focuses primarily on the pre-market side of the life cycle.

This is very much a 'medical device' standard in the traditional sense. Software is mentioned exactly once in the main body of the standard (apart from 'software' being part of the medical device definition). Annex D (which is essentially ANSI/AAMI HE74.2001, *Human factors design process for medical devices*) provides better applicability, however all the examples provided are traditional device-centric ones.

The focus is on user interaction with an independent device but lacks focus on the user interface to the 'Information' which in an inter-operable ecosystem will frequently come from other inter-connected systems. It also limits its focus to 'normal use' of the device, as it is manufacturer-oriented. The lifecycle steps would benefit from a view of the human factors risks in a broader sense than IEC 62366.

5.1.13.3 Lifecycle and granularity coverage

This standard covers the design and development lifecycle steps and is applicable at the component and application level of software.

5.1.13.4 Relationship

This standard uses ISO 14971:2007 for the identification of hazards, residual risks and other related risk terms. This standard also supplants the use of IEC 60601-1:2012, *Medical electrical equipment requirements for basic safety and essential performance*.

NOTE ANSI/AAMI HE75.2009 *Human factors engineering – Design of medical devices* complements HE74 (which is in the Appendix of IEC 62366:2007 and focuses on the HF design processes that should be in place) and contains advice from the HF/Usability world. The presentation, context and examples provided are predominately traditional medical device oriented. Useful elements of HE75, which is very large (approximately 475 pages) can be found around testing processes and a very high level overview of usability engineering principles.

5.2 Standards assessed by lifecycle applicability and software granularity

Figures 2 through 4 summarize and map each standard on the axes of lifecycle and granularity. For ease of viewing, the standards have been divided between two figures, in addition to a third figure which portrays all of the identified standards.

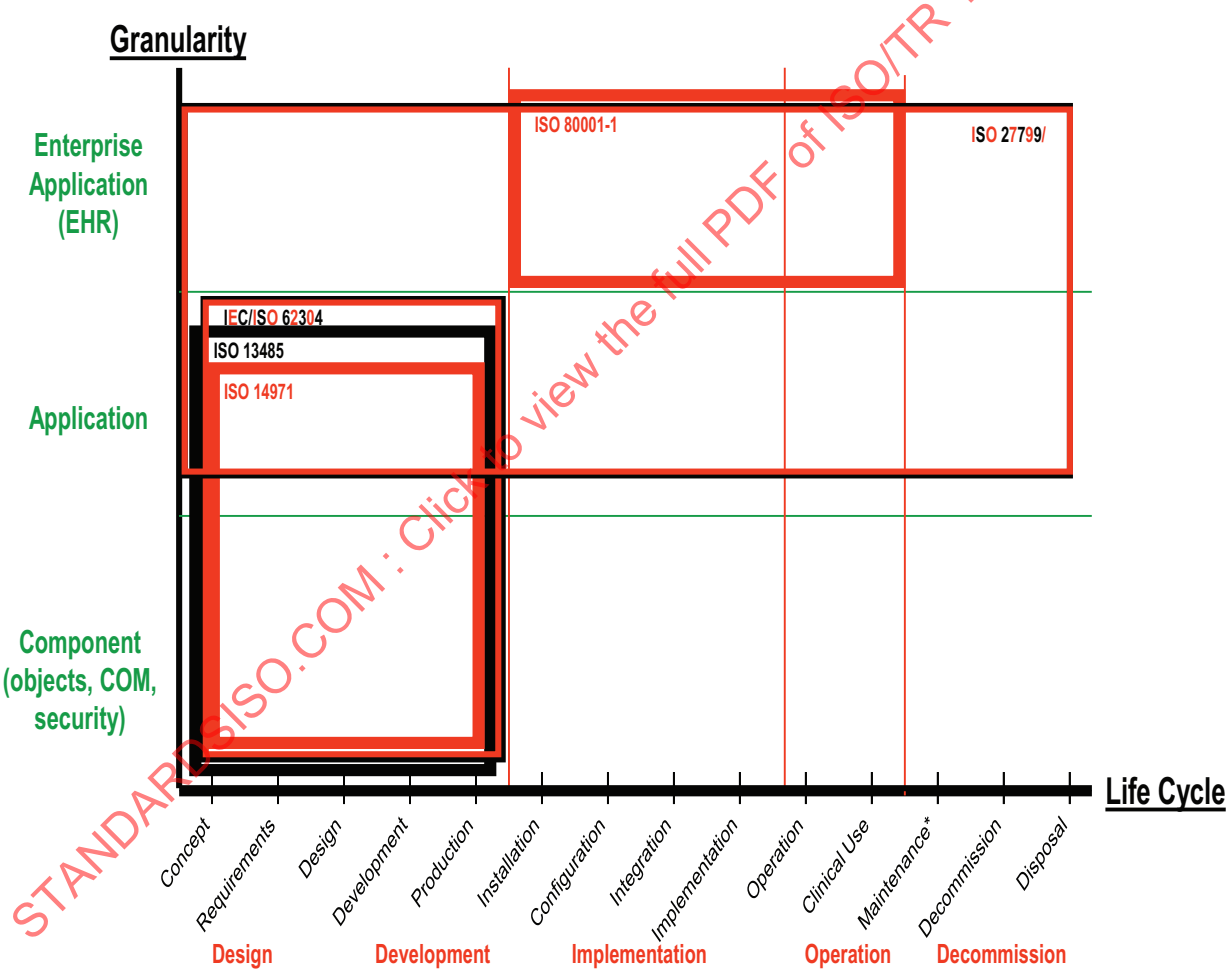


Figure 2 — Standards assessment map (covering Clauses 5.1.6 to 5.1.10)

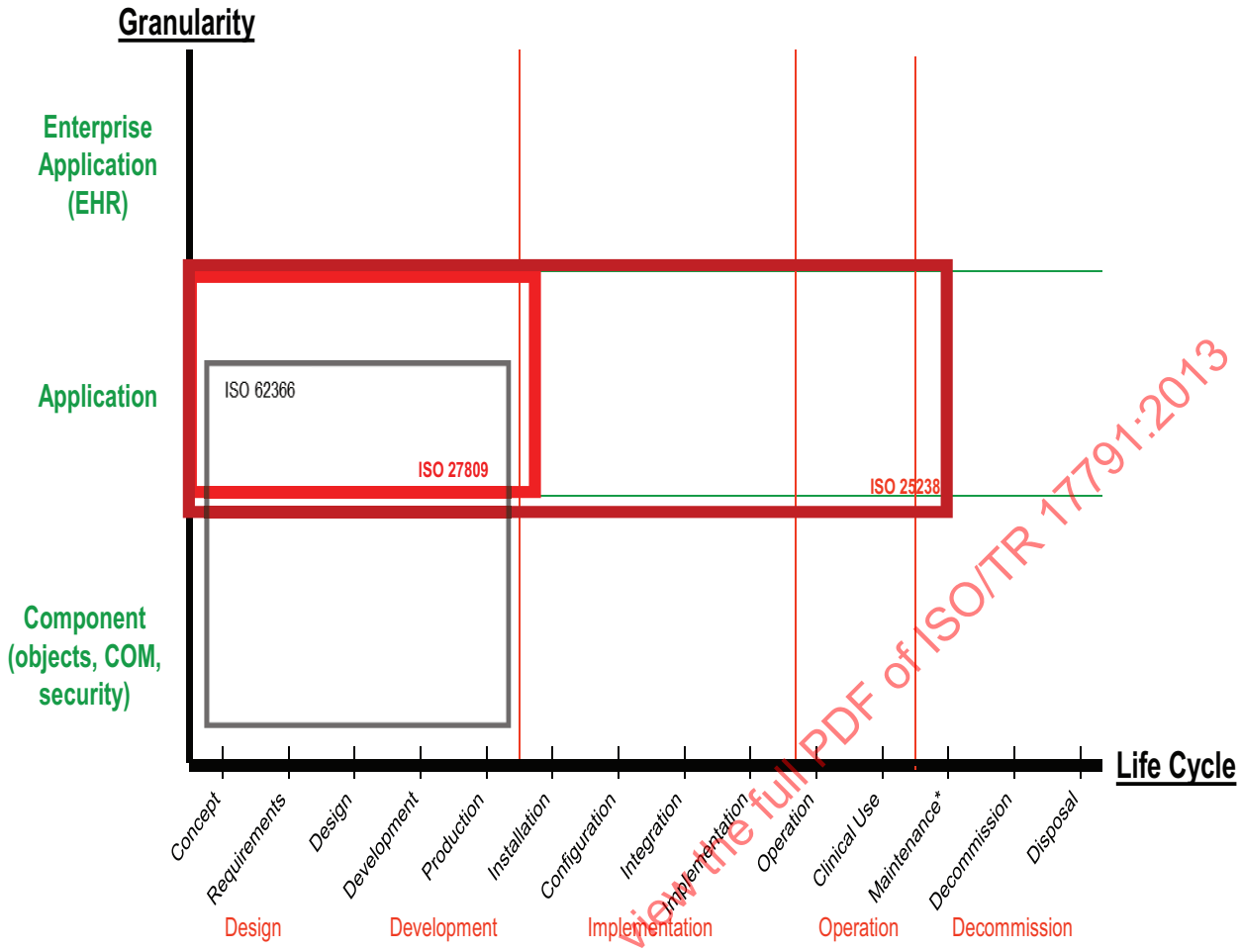


Figure 3 — Standards assessment map (covering Clauses 5.1.11 to 5.1.13)

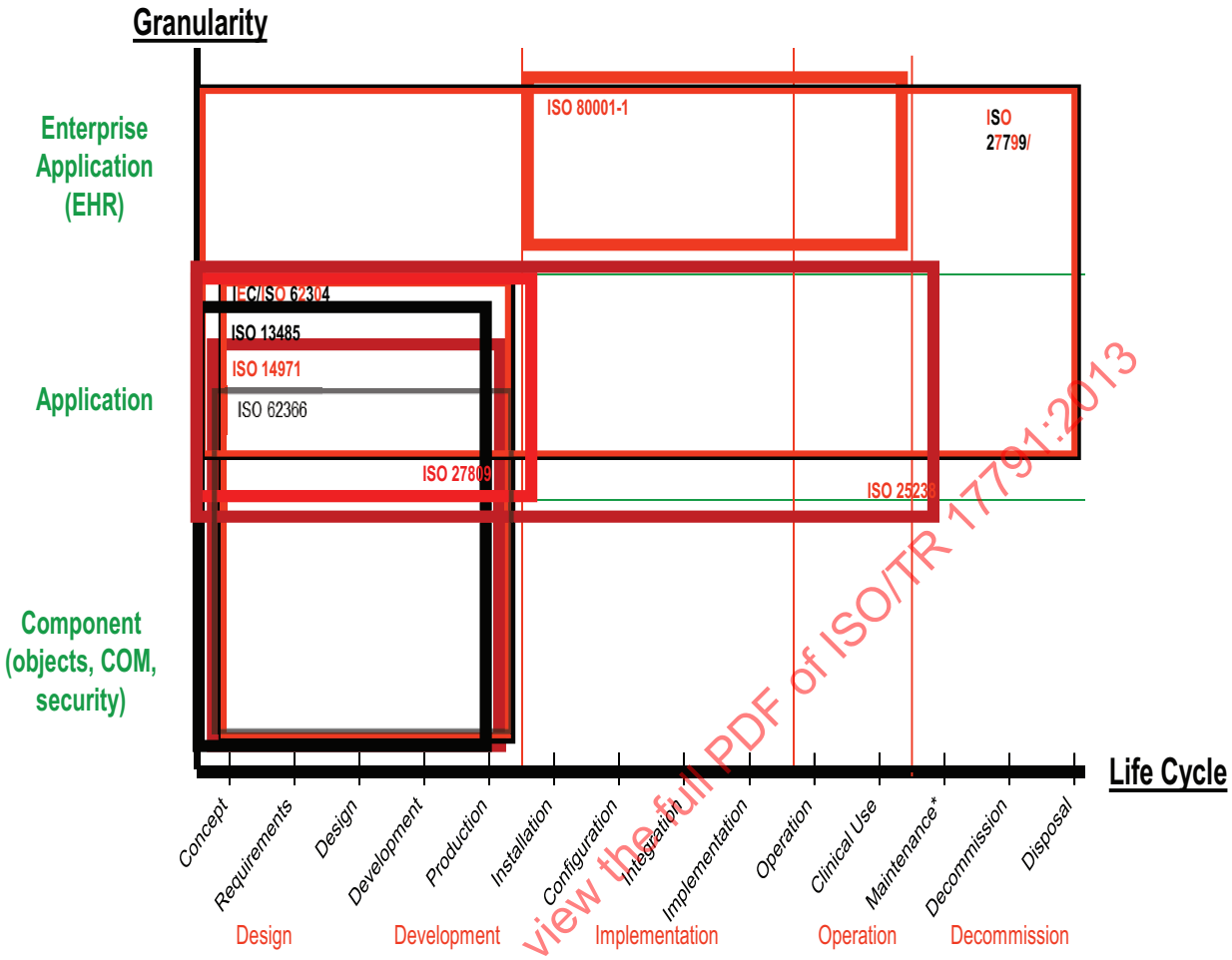


Figure 4 — Standards assessment map (covering Clauses 5.1.6 to 5.1.13)

5.3 Standards assessment overlap and gap analysis

5.3.1 General

This section describes the overlaps and gaps of the standards identified in Figure 4 in order to provide the basis for an overall assessment as to how the standards landscape could evolve to provide a more coherent approach to safe health software where:

— **overlaps** are covered in 5.3.2 to 5.3.4, providing a focus wherein multiple standards address common lifecycle stages and common software scope area, and

— **gaps** are covered in 5.3.5 to 5.3.11, providing guidance to further standards development priorities.

NOTE At the time of this Technical Report's preparation, an ad hoc group ISO/TC 215 and IEC/TC 62 SC 62A is actively working on health software related standards work items through addressing and reconciling principles, terms, and definitions.

5.3.2 ISO 13485, IEC 62304 and ISO 14971 family of medical device software-related standards

This group of standards is related by purpose and design to medical device software. ISO 13485 and ISO 14971 address the management environment that is foundational for organizations developing medical device products. ISO 13485 is focused on quality management requirements while IEC 62304 is focused on lifecycle requirements. The focus of ISO 14971 is on the application of risk management (hazards identification, risk estimation and evaluation, and risk controls).

Taken together and applied to the common design and development health software lifecycle stages, this family of standards provides guidance on enabling safety in health software.

5.3.3 IEC 62304 and ISO/IEC 12207 lifecycle standards

These two standards both address lifecycle processes while providing two different foci. IEC 62304 generically applies a quality management system focus to lifecycle components related to a manufacturer of medical device software, while ISO/IEC 12207 provides a broad, common framework with processes, activities and tasks applicable to any software: basically a roadmap of organizational processes necessary during the entire software lifecycle. Both standards apply in enabling safety in health software.

5.3.4 ISO/TS 25238, ISO/TR 27809 and ISO 14971 risk standards

These three standards provide both specific and wide-ranging risk management measures that support safety in health software.

ISO 14971 is process focused, and includes the processes to identify hazards, estimate, evaluate and control risk, and to monitor the effectiveness of medical device software controls.

ISO/TR 27809 is focused on health software control measures and the identification of associated risk management standards that provide control measures for health software applications. This Technical Report provides additional and updated material to that found in ISO/TR 27809.

ISO/TS 25238 is a risk management standard providing guidance on the classification (through analysis and categorization) of hazards and risks to patients from health software applications.

5.3.5 Gap in enterprise application process and risk standards

While the IEC 80001 series of standards seeks to address the application of risk management for IT networks incorporating medical devices, the overall health software risk and safety process domains would benefit from a targeted standard(s) reflecting best practices applicable to the increasingly complex and sophisticated environment of enterprise wide applications, with a strong emphasis on the clinical risks and related processes. Likewise, while ISO/IEC 15288:2008, *Systems and software engineering — System lifecycle processes* developed by JTC 1/SC 7 is a foundational standard for system lifecycles, it is not health software specific.

5.3.6 Gap in guidance for application of risk management to implementation, operation and decommissioning of health software

While ISO/TS 25238 and ISO/TR 27809 provide a risk focus on health software, there is a need for a specific implementation standard to provide guidance on the application of generic risk management standards to health software specifically, and also guidance on the extension and application of ISO 14971 to the implementation, operation and decommissioning of health software components and applications (supplemental to the guidance already available in IEC/TR 80002-1). Additionally, this guidance should have a strong clinical emphasis.

5.3.7 Gap in guidance on human factors for implementation and operation of health software

Current human factors standards, both internationally and country-specific, tend to focus on providing guidance to organizations on the process(es) to be followed to successfully integrate an iterative User-Centered Design (UCD) approach in the design and development of healthcare systems. Integrating a human factors approach into the design and development culture of an organization is intended to result in safer products.

ISO 9241 is a multi-part standard providing a comprehensive foundation addressing various elements of the ergonomics of human-computer interaction.

IEC 62366:2007, *Medical devices — Application of usability engineering to medical devices* and the associated ANSI/AAMI HE75.2009 *Human factors engineering — Design of medical devices* then specifies

a process for a manufacturer to analyse, specify, design, verify and validate usability as it relates to the safety of a medical device; the same processes are applicable to health software.

However, consideration of human factors during the implementation and operations stages of health software is important for other parties (system integrators, health delivery organizations, etc.) to address human factors in such areas as risk management, training, education, and roles. In particular, the team, organization and policy aspects of human factors are applicable to the implementation and the operational lifecycle stages of health software. Further guidance on this application of human factors would be useful.

5.3.8 Gap in guidance on application of safety in clinical workflow design, development, implementation and operation

While the design and development of clinical software can be guided generically with usability standards applied to medical devices, as noted above, guidance on the risk management, human factors engineering processes and quality management applied to redesign of clinical workflow is missing. There are significant risks inherent in applying health software to unassessed (and in some cases unanalysed) clinical workflow. When assessing clinical workflow, a broad, hierarchical set of human factor aspects needs to be incorporated. Additional guidance on clinical workflow documentation, analysis and redesign, and safe practices would be useful for all health software lifecycle stages.

5.3.9 Gap in guidance on code of practice for enabling eHealth safety

A comprehensive set of best practices, with appropriate clinical emphasis, needs to be identified and described that encompass a socio- technological or ecosystem approach to health software safety. Such a set would include the principles and processes useful to enable safer health software, and would provide needed guidance in this increasingly important patient safety domain, including application of the guidance in this Technical Report. Additionally, this guidance needs to have a strong clinical emphasis.

The 2011 IOM report, *Health IT and Patient Safety: Building Safer Systems for Better Care,* noted that safety is a characteristic of a socio-technical system and that system-level failures almost always occur because of unforeseen combinations of component failures.[10] This combination of component failures underscores the complexities of health software and the importance of taking a broad-based approach to applying leading practices at all software lifecycle levels and for all domains applicable (people, process, external environment, organization and technology).

5.3.10 Gap in guidance on verification and test of configuration of software

During the investigation and assessment of existing standards which could be used to ensure safer health software, it became apparent that there is a lack of guidance for the verification and testing of software configuration. Software can offer a wide variety of parameters which need to be configured according to the specific needs of the implementing organization.

Because during development not all possible variations of parameters can be tested, there is a remaining safety risk that needs to be mitigated. Guidance for implementers is needed on how to verify and test that a specific configuration is safe for the patient.

5.3.11 Gap in guidance on additional development, implementation and operational aspects of safer health software

Currently, there is no standard specific to health software that gives guidance on what is required with respect to the following in order to ensure safety of health software:

— safety related functionalities,

— non-functional characteristics, like stability, reliability, and

— labelling, including the instructions for use

all supporting the assurance of health software safety.

5.4 Standards for enabling safety in health software — Implementation and use guidance

5.4.1 General

Guidance on the available standards to support safety in health software, i.e. information that is practical, informative, implementable and useful, will be necessarily broad and of a summary nature. A definitive answer to "what standards do I use for health software safety" may be emerging but gaps need to be closed (as outlined in Clause 5.3) before a clear, comprehensive solution(s) can be realized. Pending that outcome, individuals and organizations can already take the information contained in this Technical Report and apply it to their specific contexts and circumstances to assist in understanding and advancing health software safety.

The guidance is broadly characterized in the following figure:

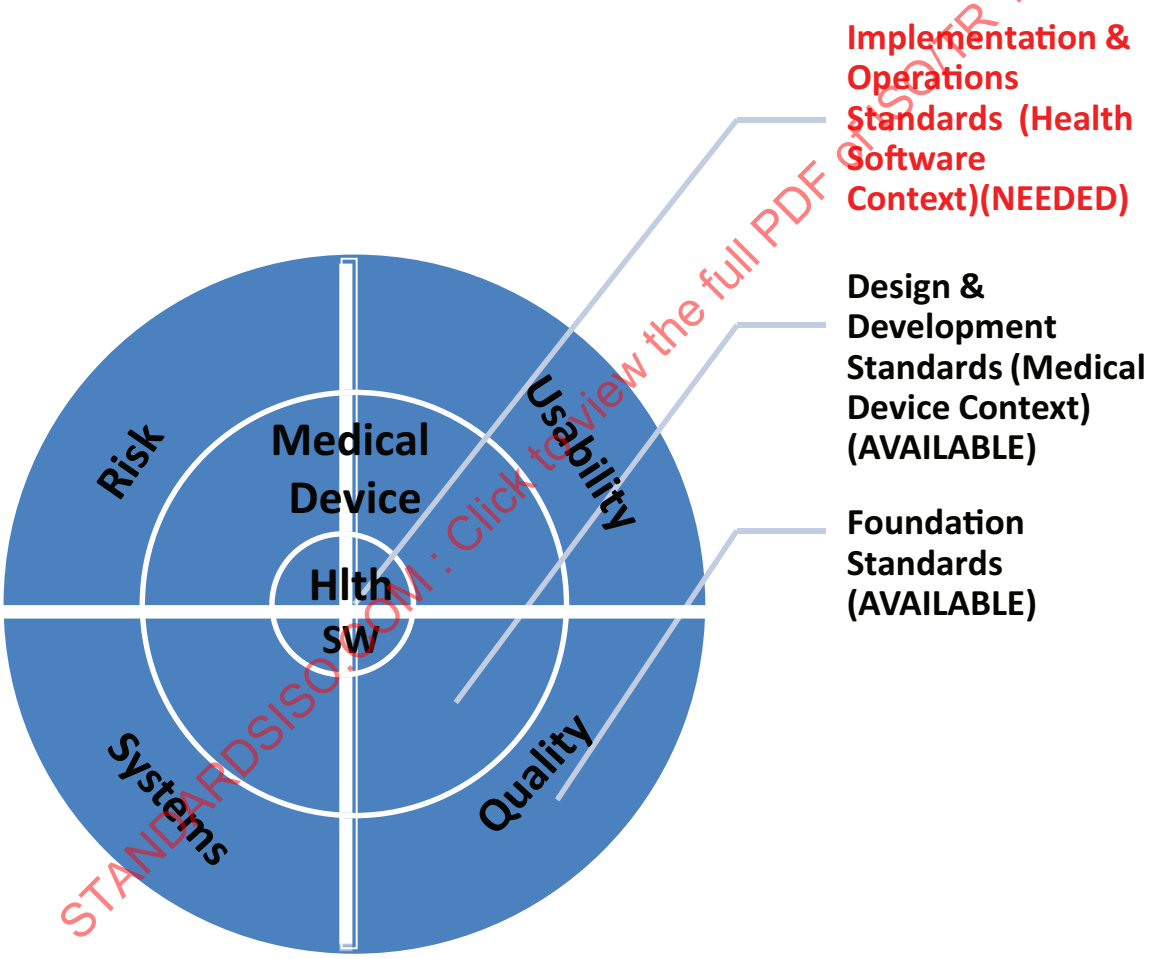


Figure 5 — Guidance on standards for safety in health software

Figure 5 reflects the following:

— Foundation standards do exist and provide a comprehensive basis for enabling safety in health software. These standards are of primary use to context specific standards developers and are also used by large software manufacturing developers.

— The standards developed from a medical device context provide a working basis for enabling safety in health software design and development.