American National Standard

AAMI HIT1000-1:202x

Safety and effectiveness of health IT software and systems—Part 1: Fundamental concepts, principles, and requirements

AAMI
Advancing Safety in Health Technology

Objectives and uses of AAMI standards and recommended practices

It is most important that the objectives and potential uses of an AAMI product standard or recommended practice are clearly understood. The objectives of AAMI's technical development program derive from AAMI's overall mission: the advancement of medical instrumentation. Essential to such advancement are (1) a continued increase in the safe and effective application of current technologies to patient care, and (2) the encouragement of new technologies. It is AAMI's view that standards and recommended practices can contribute significantly to the advancement of medical instrumentation, provided that they are drafted with attention to these objectives and provided that arbitrary and restrictive uses are avoided.

A voluntary *standard* for a *medical device* recommends to the manufacturer the information that should be provided with or on the product, basic safety and performance criteria that should be considered in qualifying the device for clinical use, and the measurement techniques that can be used to determine whether the device conforms with the safety and performance criteria and/or to compare the performance characteristics of different products. Some standards emphasize the information that should be provided with the device, including performance characteristics, instructions for use, warnings and precautions, and other data considered important in ensuring the safe and effective use of the device in the clinical environment. Recommending the disclosure of performance characteristics often necessitates the development of specialized test methods to facilitate uniformity in reporting; reaching consensus on these tests can represent a considerable part of committee work. When a drafting committee determines that clinical concerns warrant the establishment of *minimum* safety and performance criteria, referee tests must be provided and the reasons for establishing the criteria must be documented in the rationale.

A *recommended practice* provides guidelines for the use, care, and/or processing of a medical device or system. A recommended practice does not address device performance *per se*, but rather procedures and practices that will help ensure that a device is used safely and effectively and that its performance will be maintained.

Although a device standard is primarily directed to the manufacturer, it may also be of value to the potential purchaser or user of the device as a frame of reference for device evaluation. Similarly, even though a recommended practice is usually oriented towards healthcare professionals, it may be useful to the manufacturer in better understanding the environment in which a medical device will be used. Also, some recommended practices, while not addressing device performance criteria, provide guidelines to industrial personnel on such subjects as sterilization processing, methods of collecting data to establish safety and efficacy, human engineering, and other processing or evaluation techniques; such guidelines may be useful to health care professionals in understanding industrial practices.

In determining whether an AAMI standard or recommended practice is relevant to the specific needs of a potential user of the document, several important concepts must be recognized:

All AAMI standards and recommended practices are *voluntary* (unless, of course, they are adopted by government regulatory or procurement authorities). The application of a standard or recommended practice is solely within the discretion and professional judgment of the user of the document.

Each AAMI standard or recommended practice reflects the collective expertise of a committee of health care professionals and industrial representatives, whose work has been reviewed nationally (and sometimes internationally). As such, the consensus recommendations embodied in a standard or recommended practice are intended to respond to clinical needs and, ultimately, to help ensure patient safety. A standard or recommended practice is limited, however, in the sense that it responds generally to perceived risks and conditions that may not always be relevant to specific situations. A standard or recommended practice is an important *reference* in responsible decision-making, but it should never *replace* responsible decision-making.

Despite periodic review and revision (at least once every five years), a standard or recommended practice is necessarily a static document applied to a dynamic technology. Therefore, a standards user must carefully review the reasons why the document was initially developed and the specific rationale for each of its provisions. This review will reveal whether the document remains relevant to the specific needs of the user.

Particular care should be taken in applying a product standard to existing devices and equipment, and in applying a recommended practice to current procedures and practices. While observed or potential risks with existing equipment typically form the basis for the safety and performance criteria defined in a standard, professional judgment must be used in applying these criteria to existing equipment. No single source of information will serve to identify a particular product as "unsafe". A voluntary standard can be used as one resource, but the ultimate decision as to product safety and efficacy must take into account the specifics of its utilization and, of course, cost-benefit considerations. Similarly, a recommended practice should be analyzed in the context of the specific needs and resources of the individual institution or firm. Again, the rationale accompanying each AAMI standard and recommended practice is an excellent guide to the reasoning and data underlying its provision.

In summary, a standard or recommended practice is truly useful only when it is used in conjunction with other sources of information and policy guidance and in the context of professional experience and judgment.

INTERPRETATIONS OF AAMI STANDARDS AND RECOMMENDED PRACTICES

Requests for interpretations of AAMI standards and recommended practices must be made in writing, to the AAMI Vice President, Standards Policy and Programs. An official interpretation must be approved by letter ballot of the originating committee and subsequently reviewed and approved by the AAMI Standards Board. The interpretation will become official and representation of the Association only upon exhaustion of any appeals and upon publication of notice of interpretation in the Standards Monitor Online monthly newsletter. The Association for the Advancement of Medical Instrumentation disclaims responsibility for any characterization or explanation of a standard or recommended practice which has not been developed and communicated in accordance with this procedure and which is not published, by appropriate notice, as an *official interpretation* in the AAMI Standards Monitor Online.

Safety and effectiveness of health IT software and systems—Part 1: Fundamental concepts, principles, and requirements

Approved as an American National Standard on DATE by
AAMI

Abstract: Identifies the fundamental concepts and principles for creating, integrating, and implementing health IT software and health IT systems to maintain safety and effectiveness.

Keywords: health software, health IT, quality, quality systems, risk, risk management, usability, human factors engineering, safety, effectiveness, security, assurance case, safety assurance case , health IT system, sociotechnical system

Published by

AAMI
901 N. Glebe Road, Suite 300
Arlington, VA 22203-1853
www.aami.org

Printed in the United States of America

Contents

Page

Committee representation

At the time the document was published, the **AAMI Health IT Committee** had the following members:

Cochairs:
David Classen
Mark Segal

Members:
Pat Baird, Philips
Steve Binion, Becton Dickinson & Company
Rick Botney, Oregon Health & Science University
Jane Carrington, University of Arizona - College of Nursing
David Classen, University of Utah Hospital and Clinics
Richard De La Cruz, Silver Lake Group Inc
Sherman Eagles, SoftwareCPR
Neil Gardner, Alison Delle Consulting, Ltd.
John Giantsidis, CyberActa Inc.
Richard Gibson, Association of Medical Directors of Information Systems
Peter Goldschmidt, World Development Group Inc
Karoll Gonzalez, Stryker Instruments Division
William Greenrose, Deloitte
Aaron Zachary Hettinger, MedStar Health
Michael McCoy, McCoy, Lawrenceville, Georgia
Jim McGough, EdgeOne Medical
Erich Murrell, US Army Medical Material Agency
Vidya Murthy, MedCrypt
Susumu Nozawa, Siemens Healthineers
Mike Powers, Christiana Care Health Services
Mark Segal, Digital Health Policy Advisors, LLC
Rebecca Schnall, Columbia University
Jeanie Scott, Veterans Health Administration (VHA)
Elliot Sloane, Center for Healthcare Information Research and Policy
Jeffery Smith, American Medical Informatics Association
John Snyder, US Dept of Health & Human Services
Harsha Sripuram, Boston Scientific Corporation
Sharon Stanford, American Dental Association
Sandra Stuart, Kaiser Foundation Health Plan/Hospitals
Matt Weinger, Vanderbilt University Medical Center
Michael Wiklund, UL LLC
Mike Willingham, 98point6 Inc
Marisa Wilson, Alliance for Nursing Informatics (ANI)
Karen Zimmer, Independent expert

Alternates:
Elisabeth George, Philips
Andrew Gettinger, US Dept of Health & Human Services
Jeremy Jensen, Boston Scientific Corporation
Brian Pate, SoftwareCPR
Scott Robertson, Kaiser Foundation Health Plan/Hospitals
S. Vivek, ICU Medical
Nicole Zuk, Siemens Healthineers

Liaisons:
Patty Krantz-Zuppan, Medtronic Inc Campus
Beth Pumo, Kaiser Foundation Health Plan/Hospitals

Dave Osborn, Philips
Robert Phillips, Siemens Healthineers
Frank Pokrop, Sotera Wireless Inc
Diana Warner, American Health Information Management Association
Diane Wurzburger, GE Healthcare

NOTE—Participation by federal agency representatives in the development of this document does not constitute endorsement by the federal government or any of its agencies.

Foreword

Suggestions for improving this recommend practice are invited. Comments and suggested revisions should be sent to Technical Programs, AAMI, 901 N. Glebe Road, Suite 300, Arlington, VA 22203-1853 or by email to standards@aami.org.

NOTE – This foreword does not contains provisions of the HIT1000-1, *Safety and effectiveness of health IT software and systems—Part 1: Fundamental concepts, principles, and requirements*, but it does provide important information about the development and intended use of the document.

Introduction

Note: This introduction does not contain provisions of AAMI HIT1000-1:202x, *Safety and effectiveness of health IT software and systems—Part 1: Fundamental concepts, principles, and requirements,* but it does provide important information about the development and intended use of the document.

The vital role that standards for quality systems, risk management, and human factors engineering can play in enhancing the safety and effectiveness of health IT has been recognized both in the United States[1] and globally.[2] Safety and effectiveness are properties of heath IT software or systems that directly impact patient outcomes; quality systems, human factors (usability) engineering, and risk management are tools to support that safety and effectiveness of these systems across the full life cycle.

This triad (quality systems, risk management, and usability) is used successfully in many high-risk industries, including medical devices, nuclear engineering, and aeronautics. Existing general standards addressing elements of this triad (e.g., ISO 9001:2015 or ISO 31000:2018), however, are organization-focused and do not sufficiently address the complexities of the health IT world, where responsibility for safety and efficacy is shared among many different organizations and stakeholders across the product life cycle.[3] Standards for regulated healthcare technology (e.g., medical device standards, such as ANS/AAMI/ISO 13485:2016 or ANSI/AAMI/ISO 14971:2007) provide very useful concepts and direction but are developed to support regulatory compliance; applying them in the health IT sector is difficult as the regulatory status of components and systems (especially health software) and the regulatory responsibilities of stakeholders vary by product and jurisdiction.[4] There is a pressing need for standards specific to health IT that integrate key concepts and best practices from across this triad and apply them to the sociotechnical context in which health IT software and systems are deployed and used.

The AAMI HIT1000 series is intended to address this need. The standards in this series supplement existing quality management systems, risk management frameworks, and human factors engineering processes. They also facilitate shared responsibility among all stakeholders by identifying specific roles and defining the responsibilities needed to ensure health IT safety and effectiveness. The HIT1000 series provides a common framework for cooperation and collaboration among the many organizations and individuals that develop, implement, and use health IT software and systems.

The AAMI HIT1000 series (*Safety and effectiveness of health IT software and systems*) is initially comprised of the following parts:

- *Part 1: Fundamental concepts, principles, and requirements*
- *Part 2: Application of quality systems principles and practices*
- *Part 3: Application of risk management*
- *Part 4: Application of human factors engineering*

---

[1] See especially, the April 2014 *FDASIA Health IT Report: Proposed Strategy and Recommendations for a Risk-Based Framework.*

[2] See *Report of the ISO/TC 215-IEC/SC 62 Joint Task Force on Health Software* (available from International Organization for Standardization ISO/TC 215 or IEC/SC 62A, Geneva). International Standards for health IT are under development in a Joint ISO/IEC Joint Working Group (ISO/TC 215-IEC/SC 62A Joint Working Group 7). AAMI manages this Joint Working Group and is ensuring coordination between the international work and the development of the HIT1000 series. The International Standards will take several years to complete and may be considered for adoption at that time, if they may reflect the specific needs of the U.S. health IT sector. (See note 4 below.)

[3] *IOM Health IT and Patient Safety: Building Safer Systems for Better Care*. Washington DC: The National Academies Press 2012. Institute of Medicine.

[4] See *Clinical Decision Support Software: Draft Guidance for Industry and Food and Drug Administration Staff,* September 2019 (available from the FDA). In the U.S., health IT may or may not fall under medical device regulation, depending on a product's function and the risk posed to patients. The *21st Century Cures Act*, for example, removed 5 categories of software from FDA jurisdiction. In Europe, it is likely that most health IT products will fall under the European Medical Device Regulations and be treated as medical devices.

In recent years, awareness of the need for security management in ensuring the safety and availability of health IT has increased substantially, especially in response to serious and widespread security breaches (such as the WannaCry virus attacks)[5]. The AAMI HIT1000 series of provisional standards is concerned with security risks related to patient safety and effectiveness. These are addressed in the HIT1000 provisional standards as part of "safety" risk management. (See AAMI (PS)HIT1000-3:2019). Other types of security risks may be mitigated as a by-product of this risk management, but that does not obviate the need for a comprehensive security management program to ensure that the full spectrum of security-related risks is adequately addressed. Annex B of this document offers more information and useful guidance on security management.

[5] See the Health Care Industry Cybersecurity Task Force's report to Congress *Report on Improving Cybersecurity in the Health Care Industry.* (Health Care Industry Cybersecurity Task Force, U.S. Department of Health and Human Service June 2017)

Safety and effectiveness of health IT software and systems—Part 1: Fundamental concepts, principles, and requirements for patient safety

1 Scope

1.1 This series of standards and provisional standards (AAMI HIT1000 series) provides a framework for managing the safety and effectiveness of health IT software and systems, for the purpose of promoting better patient outcomes.

Note 1: Safety and effectiveness are key properties of a system. The ultimate goal of this standard is to promote patient safety and better patient outcomes. Patient safety requires systems and software that are safe and effective.

Note 2: Safety and effectiveness directly impact patient outcomes. Other attributes of software or systems, such as usability and quality, are essential to assuring safety and effectiveness and are addressed in that context by the HIT1000 series of provisional standards.

Note 3: Security-related risks are dealt with in the HIT1000 series as part of risk management. This does not obviate the need for a more comprehensive security management program to address other security risks. See Annex B for more information.

1.2 This part of AAMI HIT1000 (*Part 1: Fundamental concepts, principles, and requirements*) identifies the core concepts and principles needed to maintain safe and effective health IT software and systems. It also identifies roles and defines responsibilities, activities, and best practices that are necessary for managing that safety and effectiveness.

1.3 This standard applies throughout the whole life cycle of health IT software and systems and to all sizes and types of actors involved with that system—from developers and system integrators who create the systems, to healthcare delivery organizations (HDOs) who own, configure, implement, and use the systems, and to those responsible for operating and ultimately decommissioning health IT systems or health IT system components.

1.4 This standard defines the points in the life cycle where different roles—*Top Management, Business Owner, Developer, Integrator, Implementer, Operator,* and *User* (see Table 1)—assume primary responsibility for maintaining safety and effectiveness and identifies the communication necessary among the different roles at those points.

Note: Roles in this standard are activity-based and not dependent upon the entity or organization involved. For example, a health delivery organization may be the *Business Owner* but may also create or substantively modify health IT system components during certain stages of the health IT software and systems life cycle. At those stages, the HDO would have the role of a *Developer* and would assume the appropriate responsibilities of that role.

1.5 It is recognized that not all incorporated parts of health IT software and systems will have used this series of standards or applicable medical device software standards throughout the life cycle. Where this is the case, the safety, quality, and usability impacts of these parts must be considered and addressed so as to appropriately mitigate potential negative consequences.

Note: Other parts of the AAMI HIT1000 series can provide guidance on applying requisite vigilance to software or components that have not met the requirements of this part of AAMI HIT1000.

2 Terms and definitions

2.1
assurance
Grounds for justified confidence that a claim has been or will be achieved
[Source: ISO/IEC/IEEE 15026-1:2019]

2.2
assurance case
Reasoned, auditable artifact created that supports the contention that its top-level claim (or set of claims) is satisfied, including systematic argumentation and its underlying evidence and explicit assumptions that support the claim(s)

Note: An assurance case contains the following and their relationships:
—one or more claims about properties;
—arguments that logically link the evidence and any assumptions to the claim(s);
—a body of evidence and possibly assumptions supporting these arguments for the claim(s); and
—justification of the choice of top-level claim and the method of reasoning.
[Source: ISO/IEC/IEEE 15026-1:2019]

2.3
claim
True-false statement about the limitations on the values of an unambiguously defined property—called the claim's property—and limitations on the uncertainty of the property's values falling within these limitations during the claim's duration of applicability under stated conditions

Note 1: Uncertainties also may be associated with the duration of applicability and the stated conditions.

Note 2: A claim potentially contains the following:
—property of the system-of-interest;
—limitations on the value of the property associated with the claim (e.g., on its range);
—limitations on the uncertainty of the property value meeting its limitations;
—limitations on duration of claim's applicability;
—duration-related uncertainty;
—limitations on conditions associated with the claim; and
—condition-related uncertainty.

Note 3: The term "limitations" is used to fit the many situations that can exist. Values can be a single value or multiple single values, a range of values, or multiple ranges of values, and can be multi-dimensional. The boundaries of these limitations are sometimes not sharp, e.g. they may involve probability distributions and may be incremental.
[Source: ISO/IEC/IEEE 15026-1:2019]

2.4
effectiveness
Ability to produce the intended result
[Source: ISO 81001-1:2020]

2.5
efficiency
Resources expended in relation to effectiveness

2.6
formative evaluation
Process of assessing, at one or more stages during the HIT software or HIT system development process, a user interface or user interactions to identify the interface's strengths and weaknesses and to identify use errors that would or could result in serious harm to the patient or user
[Adapted from IEC 62366-1-:2015]

2.7
health IT (HIT)
Documented and intended application of information technology to the collection, storage, processing, retrieval, and communication of information relevant to health, patient care, and well-being
[Source: ISO 81001-1:2020]

2.8
health IT infrastructure
combined set of IT assets available to the individual or organization for developing, configuring, integrating, maintaining, and using IT services and supporting health, patient care and other organizational objectives

Note: As per the definition for asset this can include the following:
—data and information;
—health software (including medical devices, health applications, middleware, and operating system software);
—hardware components such as computers, mobile devices, servers, databases, and networks;
—services, including security, software development, IT operations and externally provided services such as data centers, internet and software-as-a-service and cloud solutions;
—people, and their qualifications, skills and experience;:
—technical procedures and documentation to manage and support the health IT infrastructure;
—HIT systems that are configured and implemented to address organizational objectives by leveraging the above assets;
—intangibles, such as reputation and image

[Source: ISO 81001-1:2020]

2.9
health IT software (HIT software)
Software intended to be used specifically for managing, maintaining, or improving health of individual persons, or the delivery of care, or which has been developed for the purpose of being incorporated into a medical device

Note 1: Health IT software consists of many components including programs, executable code, libraries, value sets, algorithms, and documentation, and is usually designed to be configurable by system integrators and health care delivery organizations to support specific business processes and use cases.
Note 2: Health IT software may be incorporated into a health IT system or may be an independent part of the technology element of the healthcare sociotechnical ecosystem if it is not integrated with other components.

[Adapted from ISO 81001-1:2020]

2.10
health IT system (HIT system)
combination of interacting health information elements that is configured and implemented to support and enable an individual or organization's specific health objectives

Note 1: Such elements include health software, medical devices, IT hardware, interfaces, data, procedures and documentation.

[Source: ISO 81001-1:2020]

2.11
human factors engineering
usability engineering
Process of applying knowledge about human behavior, abilities, limitations, and other characteristics to the design and implementation of health IT systems and software
[Adapted from IEC 62366-1:2015]

Note: For the purposes of this standard, “Human Factors Engineering” and “Usability Engineering” are identical.

2.12

incident

Event or occurrence that may cause or causes an interruption or a crisis in safety, an incident of workplace illness, or injury

[Source: World Health Organization, 2011]

2.13

life cycle

series of all phases in the life of a product or system, from the initial conception to final decommissioning and disposal

[Source: ISO 81001-1:2020]

2.14

patient safety

Reduction of risk of unnecessary harm associated with health care to an acceptable minimum [Source: World Health Organization, 2011]

Note: Patient safety, however, requires systems and software that are designed and operated in ways that reliably promote that general safety. (See. 2.19.)

2.15

quality

degree to which all the properties and characteristics of a product, process, or service satisfy the requirements which ensue from the purpose for which that product, process, or service is to be used

[Source: ISO/TS 13972:2015]

2.16

quality management systems

Set of interrelated or interacting elements that organizations use to formulate quality policies and quality objectives and to establish the processes that are needed to ensure policies are followed and objectives are achieved

Note 1: These elements include structures, programs, practices, procedures, plans, rules, roles, responsibilities, relationships, contracts, agreements, documents, records, methods, tools, techniques, technologies, and resources.

Note 2: In health care, quality of care is defined across six domains – safe, effective, patient-centered, timely, efficient, and equitable. These outcomes of care are anticipated to be better in the presence of a quality management system.

[Adapted from ISO 9001:2015]

2.17

residual risk

risk remaining after risk control measures have been implemented

[Source: ISO/IEC Guide 63:2019]

2.18

risk

Combination of the probability of occurrence of harm and the severity of that harm

Note 1: The probability of occurrence includes the exposure to a hazardous situation and the possibility to avoid or limit the harm.

[Source: ISO/IEC Guide 63:2019]

2.19

risk management

Systematic application of management policies, procedures, and practices to the tasks of analyzing, evaluating, controlling, and monitoring risk

[Source: ISO/IEC Guide 63:2019]

2.20
role
function or position
[Source: ISO/HL7 21731:2006]

2.21
safety
freedom from unacceptable risk
[Source: ISO/IEC Guide 63:2019]

2.22
safety assurance case
Assurance case (2.2) for documenting and communicating the demonstration of the validity of a safety claim by providing a convincing argument together with supporting evidence

2.23
Security (cybersecurity)
State where information and systems are protected from unauthorized activities, such as access, use, disclosure, disruption, modification, or destruction to a degree that the risks related to violation of confidentiality, integrity and availability are maintained at an acceptable level throughout the life cycle
[Source: Draft ISO 81001-1:2020]

2.24
sociotechnical system
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 is configured to support local clinical and business processes.

Note 1: The interaction and interdependence of the elements of the healthcare sociotechnical ecosystem are significant as safety is an emergent property of the sociotechnical ecosystem.

Note 2: See Figure 1.

[Source: ISO 81001-1:2020]

2.25
stakeholder
Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

Note: A decision maker can be a stakeholder.

[Source: ISO Guide 73:2009]

2.26
summative evaluation
Evaluation conducted at the end of the development process assessing user interactions with a software, device, or system interface to identify use errors that would or could result in serious harm to the patient or user

2.27
usability
Extent to which a product or system can be used by intended users to achieve their goals with effectiveness, efficiency, and satisfaction in the intended contexts of use

Note: All aspects of usability, including effectiveness, efficiency, and user satisfaction, can potentially affect safety.

[Note adapted from ISO 9241-11:2018 and ANSI/AAMI/IEC 62366-1:2015]

2.28
use environment
Actual conditions and setting in which users interact with the health IT software and system
[Adapted from ANSI/AAMI/IEC 62366-1:2015]

2.29
use error
User action or lack of user action while using the health IT software or system that leads to a different result than that intended by the developer or expected by the user

Note 1 Use errors include the inability of the user to complete a task.

Note 2 Use errors can result from a mismatch between the characteristics of the user, user interface, task, or use environment.

Note 3 A user might be aware or unaware that a use error has occurred.

Note 4 An unexpected physiological response of the patient is not by itself considered use error.

[Adapted from ANSI/AAMI/IEC 62366-1:2015]

2.30
user
Person interacting with (i.e., operating or handling) the health IT software or system

Note: Such individuals serve in a variety of roles, including administrative staff, clinical staff, regulatory staff, technical staff, or as patients.

[Adapted from ANSI/AAMI/IEC 62366-1:2015]

2.31
user interface
Means by which the user and the health IT software and system interact

[Adapted from ANSI/AAMI/IEC 62366-1:2015]

3 Context and concepts

3.1 Health IT in a complex adaptive sociotechnical ecosystem

Health IT encompasses computers, software, networks, systems, infrastructure and data operating in the context of a larger sociotechnical ecosystem that includes people, workflow, organizational factors within the healthcare delivery organization (HDO) that it is being implemented within. The HDO itself then exists within the context of the community's healthcare delivery system and external societal environment all of which have an impact (e.g. through policy, regulation, funding, etc.). This sociotechnical ecosystem (see Figure 1) is not just complex but adaptive, constantly evolving to address changes to these diverse elements.

Safety, in such a complex ecosystem, is an emergent property that depends not just on technology, but also how that technology is configured and used. When a safety issue is identified, it may be addressed within the ecosystem by adaptations, such as user workflow changes, software and system modifications, staffing adjustments, or changes in technology. The adaptive nature of the health IT software and systems is necessary, of course, but adaptations addressing the root causes are preferred and adaptations must not increase risk or raise new safety issues.

Figure 1 - Socio-technical ecosystem [Source: ISO 81001-1[6]]

Health IT software exists as part of the core technology component at the center of this sociotechnical ecosystem for an HDO. At the HDO, health software is typically incorporated into a health IT system, which contains other health IT software and IT infrastructure components. Health IT software, systems, and other supporting infrastructure (such as data centers, integration services, networks, mobile devices) are all part of this interdependent core technology component that is discussed in clause 3.2 and shown in Figure 2 below.

[6] ISO 81001-1, *Health software and health IT systems safety, effectiveness and security – Part 1: Principles, concepts, and terms*.

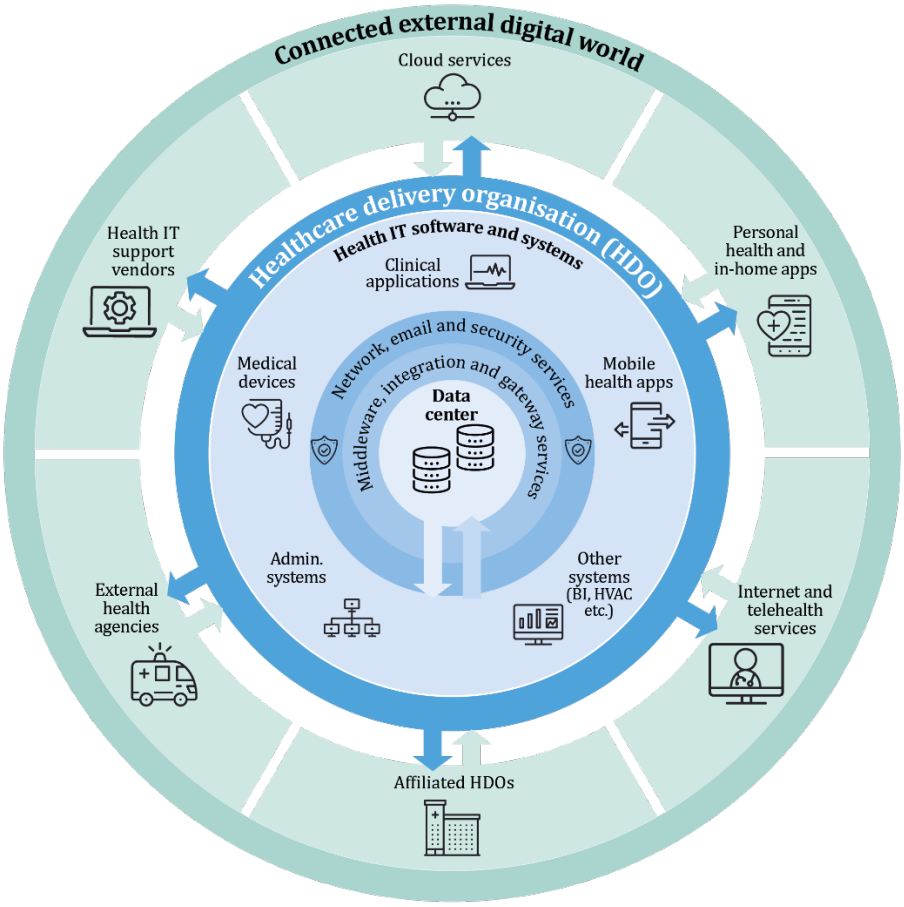

Figure 2 – System of systems [Source: ISO 81001-1[7]]

3.2 Health IT life cycles

Any distinctly identifiable health software product or system intended for healthcare or well-being is part of the technology component of the sociotechnical ecosystem. Health IT software can give instructions to hardware devices; collect, store, and manipulate data; exchange data with other systems; make treatment recommendations; or provide other functions or services. An analogy can be made that health IT software is like a living organism; it is conceived, brought into existence, matures and eventually dies. We can identify major stages of the life cycle with identifiable entry and exit criteria, and smaller steps within these stages that have less distinguishable boundaries. The health IT software progresses through the life cycle stages.

Health IT systems are composed of integrated software and hardware components assembled for a specified healthcare purpose. These systems and their components also have their own life cycle[s].

It is important to emphasize, however, that the analogy with a living organism does not hold for the sociotechnical environment. A more apt analogy would be an ecosystem (where many types of organisms exist in complex and dynamic relationships). The sociotechnical environment is dynamic and evolves and changes over time, but it cannot

[7] ISO 81001-1, *Health software and health IT systems safety, effectiveness and security – Part 1: Principles, concepts, and terms*.

be said to mature and reach an end-of-life point. Changes in the socio-technical environment, including relationships between individual components, can significantly impact health IT systems and necessitate modifications and adaptations as health IT systems move through their life cycle. Figure 2 illustrates the interdependence of medical devices, health IT software and systems within this “system of systems” in a typical health care delivery organization’s IT infrastructure.

3.3 Data management across the life cycle

Data follows a life cycle similar to that of any product; it is created, modified, and eventually deleted or archived. Incorrect or insufficient data management and oversight can result in data incompatibilities, unauthorized changes to data, loss of traceability, incomplete data, or incorrect data. These conditions can result in adverse events that are difficult to detect and analyze.

Data life cycle management activities include the following:

- monitoring and managing data formats;
- defining where and how the data is used;
- documenting who the consumers of the data are;
- documenting who is changing the data, including what changes are made to the data;
- defining valid ranges for the data; and
- auditing data quality.

The following are some methods to document data usage:

- data flow diagrams;
- data structure charts;
- control flow diagrams;
- business process mapping; and
- device to health IT software interface specifications.

The data life cycle should be fully managed and documented from creation, through modification, and to end of life.

3.4 Patient safety and health IT software and systems

There are two aspects of patient safety to consider throughout the health IT system life cycle. The first aspect is to reliably perform the processes and activities necessary for safely providing the benefits of health IT for patients (including improved safety of care in some use cases). The second aspect is to prevent the health IT system and user interactions associated with it from causing harm to patients. These are addressed by the discipline of health IT quality system management (IOM, 2012), health IT risk management, and by the application of human factors engineering throughout the health IT system’s life cycle.

3.5 Quality management and health IT software and systems

The intent of quality management is to assure that the stated and implied needs of stakeholders are consistently met. The HIT1000 series addresses patient safety. When supporting patient safety, the goal of quality management is to ensure that health IT systems are effective, efficient, satisfying to use, and free of defects.

Patient safety cannot be achieved by managing the quality of the individual components of the system alone (e.g., the health IT software). The quality of a complex system is a function of the quality of individual components, as well as their interactions. Quality management must be applied to changes in individual components, health IT systems, and the larger sociotechnical environment.

Given the interrelationships between components, and the need to manage quality, testing, and validation assessment processes should be aligned to facilitate sharing of insights and optimization of synergies.

3.6 Safety risk management in health IT software and systems

The intent of safety risk management is to prevent an unacceptable risk of patient harm due to health IT software and systems. What constitutes an unacceptable risk is determined by each organization’s risk appetite, constrained by laws,

regulations, and community norms.

Safety risk management is a process used to analyze, evaluate, control, and monitor the negative effects of health IT on patient safety during each stage of the health IT software and system life cycle. Risk management asks the questions: “what can go wrong?”; “what can you do?”; “did it work?”; “is it enough?”

Safety risk management must be applied to individual components and health IT systems.

Given the interrelationships between components, consideration of all risks must be made when a change or adaptation is judged necessary. This includes when changes are made to control identified risks. The goal of safety risk management is to proactively recognize how patient harm can occur so that the risk of that occurrence can be reduced to an acceptable level by controlling the effects that could result in that harm. This goal is the same whether the change is within the health IT system or in the context in which the health IT system is used (e.g., user interaction, workflow, clinical practice, or regulatory changes).

Information used and conclusions reached during the safety risk management process should be documented in the safety assurance case for possible use during other stages of the health IT life cycle.

3.7 Usability in health IT software and systems and human factors engineering[8]

Usability is an attribute of products and systems that can affect both safety and effectiveness. Poorly designed or implemented health IT software or system user interfaces can induce use errors, including those that lead to patient injury or death.

Therefore, as health IT systems become increasingly integral to healthcare delivery, it is important to minimize the chance of potentially harmful use errors. Not only can a product that reflects good usability principles reduce the risk of use errors and improve overall safety and effectiveness, it can also boost task efficiency and satisfy user expectations (which will encourage users to adopt and use health IT software and systems to the fullest extent).

Factors contributing to poor usability include misalignment with workflow, inadequate training or documentation, and issues with implementation. Accordingly, any such factors must be identified, assessed for potential impact on safety or effectiveness, and, if necessary, addressed in a timely manner.

The intent of applying human factors engineering to health IT is to ensure that the health IT system and software user interfaces closely align with users’ characteristics and work practices in the intended use environment. Because usability can either increase or decrease safety, applying human factors engineering when developing, customizing, and updating health IT systems and software will help ensure that health IT systems are safe, and effective, and satisfying to use.

3.8 Shared responsibility for safety

When patient safety is compromised during the configuration, integration, implementation, or operation stages, as well as because of the failure of a technology component to perform as specified in a health IT system, the developer of that component is responsible. However, patient safety may also be compromised because of unanticipated relationships between components of the health IT system or between the health IT system and the sociotechnical environment. In these cases, the responsibility for patient safety may be shared among different roles. As health IT software and systems progress through their life cycles, the primary responsibility for safety moves to different roles.

3.9 Health IT life cycle roles and responsibilities

Life cycle roles are not specific to organizations. For example, hospitals can act as developers or system integrators, and software companies can be implementers or operators. Roles are also not job titles; they are functions. A role may involve many people, or an individual may serve more than one role. Within a role many activities can be performed. These activities may be performed by one or many individuals. Refer to Table 1.

[8] See NIST GCR_15-996 – *Technical Basis for User Interface Design of Health IT* (see Wiklund et al., 2015)

485
486
487

Table 1—Life cycle roles and responsibilities

Top Management	Group of people who direct and control an organization and have overall accountability in an organization
Business Owner	The healthcare organization procuring, using, and decommissioning health IT software or health IT systems and accountable for its overall safety and effectiveness within the context of the healthcare sociotechnical ecosystem
Developer	Role responsible for execution of the the design and development phase (from concept through to release and maintenance) of a health software or health IT system. Note: A developer could be part of a manufacturer organization, a supplier of services or an HDO for example.
Integrator	Role responsible for the technical installation, configuration, data migration and integration with other health IT systems, medical devices and technology being used by the healthcare organization
Implementer	Role responsible for the clinical installation, workflow optimization and training in the clinical setting (an implementer can be the *Developer,* or *owner)*
Operator	Role responsible for keeping the health IT software or health IT system operational (and/or may be the implementers for a managed service)
User	Persons using the system in the clinical setting, which can include, for example, consumers in the case of personal health records

488

3.10 Health IT software life cycle

Figure 3 lists Health IT roles involved in the health IT ecosystem and the responsibilities associated with each role.

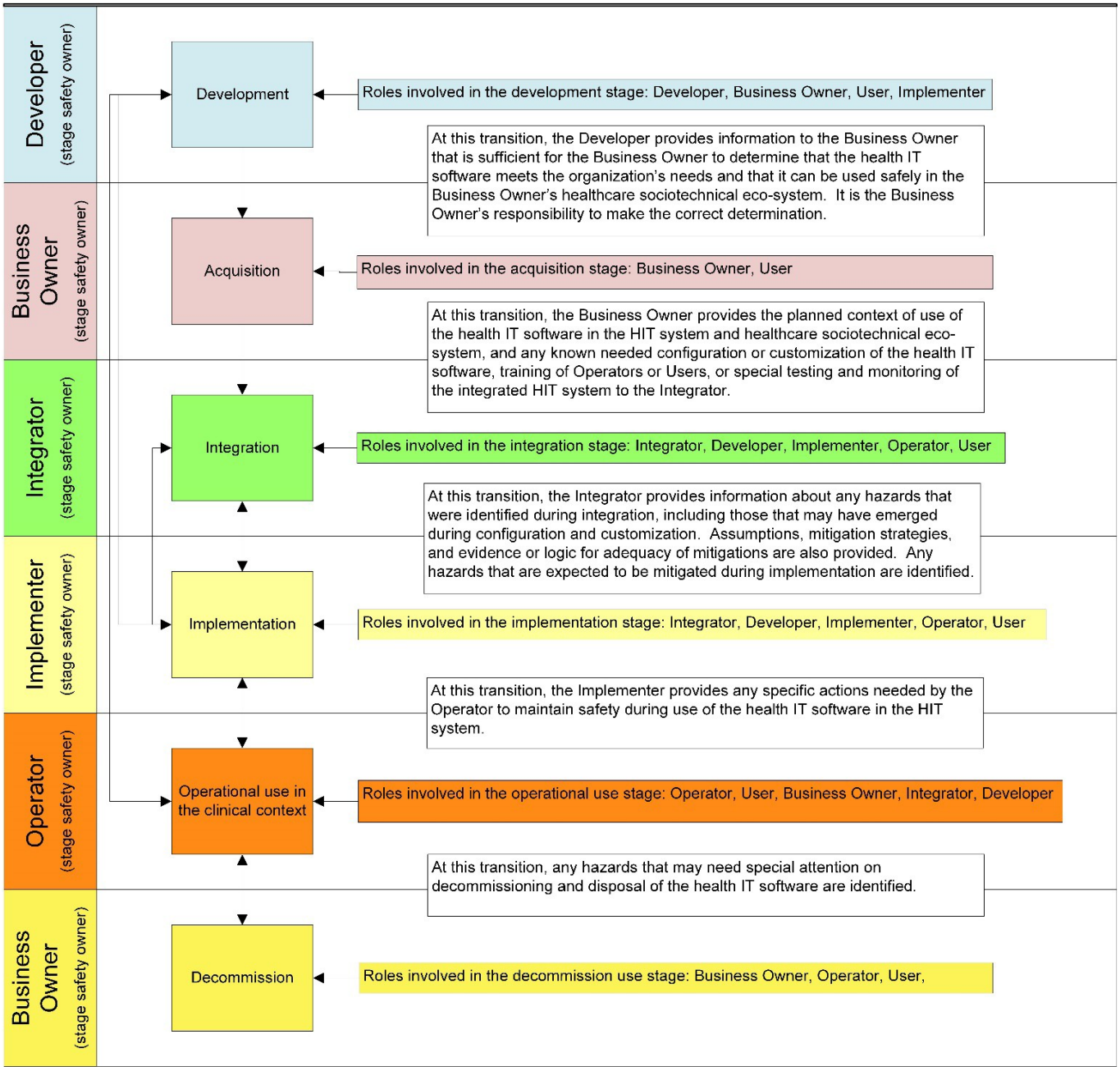

Figure 3—Health IT software life cycle stages within a HIT system (with integration and recursion possible on all paths)

3.11 Safety roles and responsibilities

Figure 3 details the health IT roles involved in the health IT ecosystem and the responsibilities associated with each role.

3.12 Transition points

As the health IT software (or health IT system that incorporates the health IT software) moves between certain life cycle stages, the primary responsibility for patient safety transitions from one role to another. While multiple roles may share responsibility, one role takes on the primary responsibility at each life cycle stage.

At these transition points, it is critical that the information necessary to continue to provide patient safety is clearly communicated and transferred to the role assuming the primary responsibility for patient safety. One way to transfer and communicate this information is via a safety assurance case, which is extended at each stage to ensure continuity in communicating essential safety information among all roles across the HIT system life cycle. The knowledge and information can be communicated by stakeholder in other ways, such as responsibility agreements or labelling.

At some transition points, such as acquisition or go-live, stage gates may be used to prevent transitions from occurring before all the necessary activities have been completed.

3.13 Activity views across the health IT software life cycle by role

A role's view identifies activities that particular role may perform looking across all stages and activities of the health IT software and systems life cycle. For example, the developer's view identifies all the activities that may be performed by a health IT software developer from concept to decommissioning of the health IT software. See Annex A for the roles that may perform the activities during each stage of the life cycle.

3.14 Applying essential health IT life cycle processes to existing systems

Just as plans should be periodically reviewed and updated (especially when system changes occur), assessments of essential health IT processes on pre-existing systems should be conducted over time as changes (or extensions) to the system are planned, or where a pattern of patient safety incidents is seen that warrants such an assessment.

3.15 Health IT system risk benefit analysis

Health IT system safety risk benefit analysis is used when the residual safety risk associated with a hazard is judged unacceptable. The safety risk benefit analysis weighs the expected clinical benefit against the possible patient harm. The decision as to whether the residual risk is outweighed by the benefits provided is essentially a matter of judgement by experienced and knowledgeable individuals, which would normally include the Health IT Safety Owner and a Clinical Safety Officer. Unfortunately, there is no accepted standardized approach to estimate clinical benefit, and a greater degree of variation will be the inevitable result of using different approaches.

Those involved in making health IT system risk benefit judgements have a responsibility to understand and consider the technical, clinical, regulatory, economic, sociological, and political context of their risk management decisions. For a healthcare delivery organization, this will include understanding and considering the enterprise benefits that apply to a population, as well as the benefits to individual patients.

If the analysis does not support the conclusion that the clinical benefits outweigh the residual health IT system risk, then the health IT system risk remains unacceptable. Generally, if all practicable health IT system risk control measures are insufficient to satisfy the health IT system risk acceptability criteria, then approval to deploy and use the system (or the functionality that is problematic) should not be granted.

Proceeding to the next stage with health IT software or a health IT system that retains unacceptable risk requires explicit approval by Top Management using established governance processes. In such a case, the health IT system risk must be communicated across the health organization to ensure full awareness.

The health IT system risk benefit analysis needs to be documented in the health IT system Safety Assurance Case

report and whether the residual health IT system risk is now acceptable needs to be documented.

3.16 Safety assurance case

A safety assurance case provides the documented evidence to support a convincing argument that a health IT system can be implemented safely for its intended use. It identifies the applicable hazards, hazardous situations and causes, and demonstrates why the specific risk controls chosen are adequate, individually effective, and collectively sufficient to reduce the overall residual risk to an acceptable level. While the decision on how to make the argument can be flexible and tailored to the situation, it should reference all supporting material in a clear, comprehensible, and concise format.

The safety assurance case continues to evolve through the health IT system life cycle and will require updating by the organization responsible for each stage as the system moves towards implementation and use. Updates should be based on the further details of the specific context of the health IT system's expected use, as well as the known and emergent hazards and the corresponding risk controls designed to address them. The safety assurance case plays a vital role in ensuring that the necessary information is communicated at the transition points and facilitates shared responsibility by supporting the decision to transition to the next phase from a safety perspective. It also can provide and communicate the necessary clinical assurance to the end users and top management and, where appropriate, to other stakeholders.

A safety assurance case provides the following:

- a summary of all the relevant knowledge that has been acquired relating to the clinical risks associated with the health IT system at that point in the life cycle;
- a clear and concise record of the process that has been applied to determine the clinical safety of the health IT software and system;
- a summary of the outcomes of the assessment procedures applied;
- a clear listing of any residual clinical risks that have been identified, and the related operational constraints and limitations that are applicable;
- a clear listing of any hazards and associated clinical risks that are being transferred to the next stage in the life cycle, together with any declared risk control measures that are to be addressed by the responsible organization for that stage; and
- a listing of outstanding test issues/defects associated with the health IT system which may have a clinical safety impact.

4 Principles

4.1 Quality management principles

4.1.1 General

Quality management principles (QMPs) are a set of fundamental beliefs, norms, rules, and values that are accepted as true and can be used as a basis for quality management. This standard uses a set of seven QMPs [see 4.1.2. – 4.1.8] that were developed and updated by international experts of ISO/TC 176—the International Committee responsible for developing and maintaining ISO's quality management standards [e.g., ISO 9001:2015]. Such QMPs can be used to guide an organization's performance improvement. These principles are not listed in priority order. The relative importance of each principle will vary from organization to organization and can be expected to change over time. These principles apply to every organization that is involved in developing, implementing and operating health IT software or a health IT System.

4.1.2 Customer and stakeholder focus

Sustained success is achieved when an organization attracts and retains the confidence of customers and other interested parties. Every aspect of customer interaction provides an opportunity to create more value for the customer. Understanding current and future needs of customers and other interested parties contributes to sustained success of the organization. A central promise of health IT has been improved patient safety, so the principal customer focus is on both the healthcare provider and the patient. The patient focus should include situations where patients contribute, consume, and share their health information.

4.1.3 Leadership

Creation of unity of purpose and direction and engagement of people enable an organization to align its strategies, policies, processes, and resources to achieve its objectives. Leadership includes sponsoring and communicating quality objectives and goals, setting examples, providing people with the required resources, training and authority to act with accountability, and inspiring, encouraging, and recognizing individual contributions.

4.1.4 Engagement of people

Recognition, empowerment, and enhancement of competence facilitate the engagement of people in achieving the organization's quality objectives. It is critical to promote collaboration throughout the organization and facilitate open discussion and sharing of knowledge and experience.

4.1.5 Process approach

The quality management system consists of interrelated processes. Understanding how results are produced by this system enables an organization to optimize the system and its performance. Processes and their interrelations as a system should be managed to do the following:

a) achieve the organization's quality objectives effectively and efficiently;
b) ensure that the information necessary to operate and improve the processes and monitor, analyze, and evaluate the performance of the overall system is available; and
c) manage risks that can affect outputs of the processes and overall outcomes of the quality management system.

4.1.6 Improvement

Improvement is essential for an organization to maintain current levels of performance, to react to changes in its internal and external conditions, and to create new opportunities to improve patient safety. Organizations should integrate improvement considerations into the development of new or modified goods, services, and processes. They should also track, review, and audit the planning, implementation, completion, and results of improvement projects.

4.1.7 Evidence-based decision making

Decision making can be a complex process, and it involves some uncertainty. It often involves multiple types and sources of inputs, as well as their interpretation, which can be subjective. It is important to understand cause-and-effect relationships and potential unintended consequences. Facts, evidence, and data analysis lead to greater objectivity and confidence in decision making. The objective is to make decisions and take actions based on evidence, balanced with experience and intuition. Making decisions based on evidence requires that the organization determine, measure, and monitor key indicators to demonstrate the organization's performance and ensure that data and information are sufficiently accurate, reliable, and secure. The required data should be available to the relevant people.

4.1.8 Relationship management

Interested parties influence the performance of an organization. Sustained success is more likely to be achieved when the organization manages relationships with all of its interested parties to optimize their impact on its performance. Relationship management with its supplier and partner networks is of particular importance. Each organization should determine and prioritize interested party relationships that need to be managed, establishing relationships that balance short-term gains with long-term considerations. Organizations should pool and share information, expertise, and resources with relevant interested parties; measure performance and provide performance feedback to interested parties, as appropriate, to enhance improvement initiatives; and establish collaborative development and improvement activities with suppliers, partners, customers, and other interested parties.

4.2 Risk management principles

Note: The risk management principles are taken from ISO 31000:2018, *Risk management – Framework and process – Guidelines.*

4.2.1 General

The principles provide the basis for the management of risk, communicate the value, the intention, and purpose of risk management. If these principles are considered, then an organization is more likely to manage risk successfully and meet its objectives.

4.2.2 Value creation and protection

Risk management creates and protects value. It contributes to the demonstrable achievement of objectives, innovation, and improvement of performance in, for example, human health and safety, security, legal, and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance, and reputation.

4.2.3 Integration

Risk management should be integrated into all organizational activities and decision making. It is not a stand-alone activity that is separate from the activities and processes of the organization. Everyone in an organization has responsibility for managing risk. Risk management improves decision making at all levels.

4.2.4 Structured approach

Risk management is systematic and structured. A systematic and structured approach to risk management contributes to efficiency and to consistent, comparable, and reliable results.

4.2.5 Customized

The framework and processes to manage risk are tailored to the organization's external and internal context, objectives, and risk profile. Each organization's unique structural arrangements, management accountabilities, and performance metrics are the basis for designing and aligning the risk management framework and processes.

4.2.6 Inclusive

Risk management is inclusive. Appropriate and timely involvement of stakeholders enables their knowledge, views, and perceptions to be considered, which results in improved awareness and informed risk management and decision making.

4.2.7 Dynamic and responsive

Risk management is dynamic and responsive to change. Risks may emerge, change, or disappear as a result of changes and events in an organization's internal and external context of operations. Risk management should adopt a proactive approach that detects, acknowledges, and responds to those changes in a timely manner.

4.2.8 Best available information

Risk management should be based on the best available information. The inputs to the process of managing risk are based on information sources, such as current and historical data, experience, stakeholder feedback, observation, forecasts, and expert judgement. Decision makers should consider any limitations and uncertainties of the data, modelling, and divergence among experts.

4.2.9 Human and cultural factors

Risk management takes human and cultural factors into account. Human behavior and culture significantly influence all aspects of risk management at each level and stage. Risk management should consider the variability of human behavior and culture, such as values, perceptions, beliefs, attitudes, intentions, competencies, and capabilities.

4.2.10 Continual improvement

Risk management facilitates continual improvement. Risk management improves organizational performance through increasing awareness and developing capabilities based on continuous learning and experience. These activities support organizational learning and resilience.

4.3 Human factors engineering principles

Note: The principles below summarize best practices for applying human factors engineering (usability engineering) to health IT software and health IT system development and implementation. These principles are adapted from NIST GCR 15-996 – *Technical Basis for User Interface Design of Health IT* (see Wiklund et al. 2015).

4.3.1 General

Developers should establish and maintain a human factors engineering process, such as outlined in AAMI HIT1000-4(PS):2020. Key components of the process include the following: determining user needs; identifying opportunities for improved efficiency and effectiveness; identifying potential use errors; determining use-related risks; establishing user interface requirements; designing the user interface; conducting formative usability tests; and conducting summative (i.e., validation) usability tests.

Developers should iterate the design process (e.g., *establish user interface requirements → design → model → test)* to the extent necessary to ensure the system's usability. Further, the human factors engineering process should span the entire product life cycle, including post-deployment monitoring.

4.3.2 Collaboration during the development process

Developers should invest in professional usability expertise and encourage frequent interaction between usability experts and development teams. A collaborative, open dialogue between the development team and dedicated usability experts promotes the integration of human factors engineering into the development process.

4.3.3 Use-related risk management process

The human factors engineering process should be applied in parallel to a use-related risk management process, which details and analyzes related risks, ensuring that the product does not enable users to commit a safety-related use error or that the risk associated with such use errors is mitigated to the greatest possible extent. Developers should convene a dedicated, multidisciplinary team to consider, eliminate, or mitigate sources of use-related risk.

4.3.4 Organizational value

Strong leadership support for human factors engineering within health IT software and system development, distribution, and management organizations helps build a culture that values and prioritizes human factors engineering principles and activities. Leadership should ensure they are well-informed regarding basic human factors engineering principles and their effect on the health IT system's usability, use safety, and commercial success.

4.3.5 User input

Developers should establish and maintain a diverse user base, enabling them to obtain rapid feedback throughout the design and development process, as well as to identify and address usability issues that occur after implementation. Organizations should engage the user base to participate in regular user research activities and identify a core group of users representing diverse demographic characteristics and clinical specialties.

4.3.6 Clinical expertise

Considering typical and optimal user workflows and clinicians' mental models of frequent, urgent, and critical tasks will increase product efficiency, usability, and user satisfaction. As such, developers should collaborate with representative users to draft user profiles and use cases to better understand users, tasks, and workflows. Additionally, further investigating users' typical workflows will help develop an understanding of the cognitive requirements of particular tasks, users' mental models of particular tasks, and the nature of user collaboration and interaction.

4.3.7 Usability engineering activities

Conducting a variety of human factors engineering (i.e., user-centered design) activities helps developers form a multi-faceted understanding of user interactions with the product. Organizations should plan human factors engineering activities that provide relevant and appropriate input during particular phases of the design and development process, as well as at key junctures throughout the health IT system life cycle (e.g., shortly after implementation and after major system updates).

4.3.8 Formative and summative evaluations

Conducting multiple formative [2.6] tests in the early stages of the design process, and using test findings to inform product development, facilitates safe and usable health IT system design. Organizations should allocate resources to formative usability testing throughout the product development life cycle, focusing on phases in which study findings can still inform health IT system design and design changes are less costly (i.e., relative to later-stage testing). Finally, summative evaluations [2.26] should be conducted before implementation to ensure that the product is safe and effective for use by the intended users in the intended use environments.

5 Fundamental requirements

5.1 Application

These requirements apply to every organization that is involved in developing, implementing and operating health IT software or a health IT system.

5.2 Essential health IT life cycle processes (quality, risk, and human factors)

During each stage of the health IT life cycle, quality management, risk management, and human factors engineering processes shall be defined. The Health IT Safety owner of that stage shall ensure that the personnel who must implement these procedures are familiar with them and are implementing them correctly.

5.3 Competencies of personnel

5.3.1 Personnel shall have the knowledge, experience, and competencies appropriate to undertake the tasks assigned to them.

5.3.2 Competency and experience records for the personnel involved in performing the tasks shall be maintained.

5.3.3 Top Management shall monitor the performance of health IT software or a health IT system to assure that it is functioning safely and effectively.

5.4 Top management responsibilities

5.4.1 In executing the health IT processes for a given life cycle stage, Top Management, at a minimum, shall do the following:

a. make available sufficient resources at an organization-level to implement roles and responsibilities as identified in this standard appropriately;
b. assign competent personnel from each of the specialist areas that are involved in assuring the safety of the Health IT Software or health IT System; and
c. appoint a Health IT Safety Owner.

5.4.2 Top Management shall ensure that appropriate levels of authorization for the health IT software or health IT System and its safety documentation are defined.

5.5 Health IT safety owner

5.5.1 A Health IT Safety Owner shall be suitably qualified and have clinical workflow and systems knowledge.

5.5.2 A Health IT Safety Owner shall have appropriate information systems knowledge.

5.5.3 A Health IT Safety Owner shall be knowledgeable in quality and risk management and their application to health IT domains.

5.5.4 A Health IT Safety Owner shall make sure that the processes defined for health IT are followed.

5.6 Products not intended for the purpose of affecting human health and health care

Any product that is included within health IT software or a health IT system that was not developed for the purpose of directly affecting human health and health care (e.g., a database system or a registration or scheduling system) shall be assessed for quality and safety that could impact clinical care. If the failure of the product to perform as expected could cause harm, the risk of the harm shall be managed.

5.7 Monitoring, surveillance, reporting and management

Each organization shall monitor and formally review its health IT processes at planned, regular intervals, and as necessary, based on results of routine monitoring of health IT software or health IT system performance.

Given the increasing complexity of health IT software and systems, and the many potential sources of errors from within the sociotechnical ecosystem, an active approach to surveillance, reporting, and incident management is also needed to detect, anticipate, and respond to actual and potential patient safety incidents.

a) A broad range of measures covering areas such as user adoption, satisfaction, service desk logs, system responsiveness, data quality, adherence with decision support recommendations, and security should be incorporated into an active surveillance program.

b) Incidents will occur, and it is important that any incidents (including near misses) are identified by all staff involved in designing, supporting, or using the system (or its data) without fear of retribution or being held responsible as the source of the error. Incidents shall be managed through a pre-defined process, such as root cause analysis, so that the safety owner(s) can promptly investigate incidents and take any necessary corrective action to prevent or mitigate further harm.

c) It is important that these incidents be reported and communicated to all appropriate parties in a transparent way so that any necessary action can be taken to reduce the likelihood or consequences ofre-occurrence.

d) Documentation of the incident, the results of its investigation and any corrective actions that were needed shall then be recorded in a database that can then be promptly accessed to aid in investigating and addressing future incidents that appear similar.

e) This could include prospective techniques such as post-implementation surveillance.

6 Documenting health IT safety

6.1 These requirements apply to every organization that is involved in developing, integrating, implementing, and operating health IT software or a health IT System. Each stage (development, integration, implementation, operation) should have its own documentation that includes, at a minimum, the following:

a) assumptions and decisions made that influence the health IT quality management and risk management activities;
b) a record of hazards identified;
c) a health IT safety assurance case, as defined earlier in this standard, addressing the identified hazards; and
d) a health IT safety assurance case report. (When the Primary Safety Owner[9] changes at a risk management transition point, a health IT Safety Assurance Case report or similar documentation shall be provided to the successor Primary Safety Owner).

6.2 As the health IT software advances through its life cycle, its safety assurance case is incorporated into the health IT system safety assurance case and the safety assurance case for using the health IT system in the larger health IT sociotechnical ecosystem.

[9] See AAMI HIT1000-3(PS): 2019.

Annex A
(normative)

Health IT software life cycle stages and activities

The stages of the health IT life cycle are listed below. It should be noted that the stages and activities may be iterative and are not necessarily sequential. In most cases, activities may occur concurrently, but complete sequentially. Risk management is performed throughout the life cycle and is documented in a Safety Assurance Case. This table is illustrative and not necessarily comprehensive.

Table A1—Health IT software life cycle stages and activities

Note: See 3.9 for discussion of the life cycle roles and Figure 2 for the software life cycle stages within a health IT system. Life cycle stages in this table and Figure 2 are color-coded.

Life cycle stage	Life cycle Activities	Step definition and activities needed during the step	Role(s) involved in activity
Development		Design and development are a process (or a set of processes) using resources to transform requirements (inputs) into characteristics or specifications (outputs) for products, processes, and systems.	Developer
	Concept/ requirements	Conceiving, imagining, and specifying the initial design of the aesthetics and primary functions of the software	Developer, User
	Requirement analysis	A requirement is a need, expectation, or obligation. It can be stated or implied by an organization, its customers, or other interested parties.	Developer
	Task analysis	Process in which all potential user interactions with the software are analyzed as a means to identify potential use errors, particularly those with the potential to cause significant harm The task analysis should serve as the foundation for risk control and risk management activities.	Developer
	Design	A design is concerned with how the problem is to be resolved.	Developer
	Development	The design is transformed into a product, process, or system.	Developer
	Formative Evaluation	Conduct formative usability evaluations throughout the development processes and use	Developer

		the results to improve the system's design/efficacy.	
	Verification	The output of the development step is reviewed, inspected, or tested to establish and document that it correctly implements the requirements.	Developer
	Summative Evaluation	Conducting summative evaluations on the product-equivalent system	Developer
	Delivery	A release is a specific version of a product, service, or system that is made available by distribution to owners or implementers for a particular purpose.	Developer, Business Owner, Implementer

Transition point from *Developer* to *Business owner*

At this transition the Developer provides information to the Business Owner that is sufficient for the business owner to determine that the health IT software meets the organization's needs and that the Safety Assurance Case demonstrates the software can be used safely in the Business Owner's healthcare sociotechnical ecosystem. It is the Business Owner's responsibility to make the correct determination.

Life cycle stage	Life cycle Activities	Step definition and activities needed during the step	Role(s) involved in activity
Acquisition	Procurement	Defining requirements and acquiring a solution to meet the organization's needs through an available product, or engaging an organization for the production of "bespoke or in-house developed" products	Business Owner

Transition point from *Business Owner* to *Integrator*

At this transition, the Business Owner provides the planned context of use of the health IT software in the health IT system and healthcare sociotechnical ecosystem, and any known configuration or customization of the health IT software, training of operators or users, or special testing, and monitoring of the integrated health IT system to the Integrator.

Life cycle stage	Life cycle Activities	Step definition and activities needed during the step	Role(s) involved in activity
Integration	Installation	Software conformance testing and certification may also be included in the integration step, either as a first or pre-installation step.	Integrator, Developer, Implementer, Operator
	Configuration	Configuring the health IT software and other supporting components of the health IT system to address the organization's specific requirements	Integrator, Developer

	Customization	Modifications or additions to the health IT software or other components of the health IT system that require customized coding (as they cannot be addressed through configuration)	Integrator, Developer
	Integration	Connection of the health IT software with the other health IT system components (e.g., to allow for data exchange or validation)	Integrator
	Data extraction and transformation	Transforming and loading source data into the appropriate tables in the health IT system	Integrator
	Integration testing	Testing the configuration, integration, or interfaces between components of the health IT system (e.g., between different components, such as the operating system, file system, and hardware, as well as interfaces with other health IT systems with which the health IT software needs to communicate)	Integrator

Transition point from *Integrator* to *Implementer*

At this transition the Integrator provides the Implementer additional information in the Safety Assurance Case about any hazards that were identified during integration, including those that may have emerged during configuration and customization. Assumptions, mitigation strategies, and evidence or logic for adequacy of mitigations are also provided. Any hazards that are expected to be mitigated during implementation are identified.

Life cycle stage	Life cycle Activities	Step definition and activities needed during the step	Role(s) involved in activity
Implementation	Workflow assessment and optimization	Assessing the current clinical and business workflow and identifying how the new health IT software should be optimally used in meeting each affected organizational unit's objectives	Implementer, User
	Decisio n support	Confirming that decision support rules in the system align with clinical best practices and expectations for the targeted organizational environment(s)	Implementer, User
	Patient identification and data quality	Ensuring that the system facilitates the accurate identification of patients and the capture, storage, interpretation and communication of accurate patient information	Implementer, User
	Change manageme nt and training	Preparing the end user environment for accepting the work process changes and supporting users in utilizing the new system safely and effectively	Implementer, User
	Pre-roll-out testing.	Implementing the system in a pre-production test environment so that end users can do a	Implementer, User

		final test of all functions of the system using 'real world' scenarios	
	Pilot or limited production roll- out	Implementing the system in a small number of user production environments to assess and ensure the system's readiness	Implementer, User
	Go-Live	Making the system fully active so that its intended users can access and utilize it in carrying out the full range of targeted functions Note: Depending on the scale of the implementation, the Go-Live stage may involve a staged roll-out in order to ensure the variety of end user environments can be adequately supported.	Implementer, Operator, User
Transition point from *Implementer* to *Operator* At this transition the Implementer documents any specific actions needed by the Operator to maintain safety during use of the health IT software in the health IT system and any hazards that may need special attention during decommissioning and disposal of the health IT software in the Safety Assurance Case.			
Life cycle stage	**Life cycle Activities**	**Step definition and activities needed during the step**	**Role(s) involved in activity**
Operational Use in the clinical setting	Post-deployment monitoring	Monitoring and optimizing network, database, infrastructure support to the health IT system	Operator
	Surveillance and monitoring	Includes active monitoring of the system's use in the clinical setting through measures such as user satisfaction, data quality, and the effectiveness of critical functions such as decision support, as well as ensuring any safety incidents are identified and analyzed with appropriate remediation (including reporting to appropriate parties) to reduce the likelihood of future re-occurrence	Operator, Developer, Business owner
	Modification and maintenance	Modification or maintenance of health IT software or the health IT system after delivery to correct faults, improve or assure technical performance or other attributes, or to add, improve or restore functionality, accuracy, timeliness, integrity, usable for purpose	Developer, Integrator, Operator, User

Transition point from *Operator* to *Business owner*

At this transition the Operator documents any specific actions needed by the Business Owner to maintain safety during decommissioning of the health IT software in the health IT system and any hazards that may need special attention on decommissioning of the health IT software in the safety assurance case.

Life cycle stage	Life cycle Activities	Step definition and activities needed during the step	Role(s) involved in activity
Decommission		Retiring and ending the existence of a system's existing software products or services while preserving the integrity of organizational operations The system is removed from the operational environments, and system work products and data are archived in the appropriate manner.	Business Owner, Operator, User

Annex B
(informative)

Useful guidance on security management for health IT software and systems

B.1 Introduction and discussion

Security is important for maintaining the safety and effectiveness of health IT systems and software. Security risks however, are broader than just those affecting effectiveness and patient safety; they include risks to confidentiality and privacy, as well as larger enterprise risks (e.g., financial, reputational, operational). The AAMI HIT1000-1 series of provisional standards is concerned with security risks related to patient safety. These are addressed in the HIT1000 provisional standards as part of “safety” risk management (see AAMI (PS)HIT1000-3:2019). Other types of security risks may be mitigated as a by-product of safety risk management, but this does not obviate the need for a comprehensive security management program to ensure that the full spectrum of security- related risks is adequately addressed. Addressing security in a comprehensive way also helps to protect the confidentiality, integrity, and availability of the larger healthcare infrastructure.

Methods and best practices for managing security in its various forms are well-characterized in many different publications, standards, and technical documents (see B.3 for a bibliography of resources). It is essential that healthcare facilities and health IT developers have established procedures and processes for addressing all security risks. It is also important that they have open communication with the other stakeholders to ensure proper coordination and information around managing emergent security threats.

B.2 Guidance on security engineering

B.2.1 General

The following guidance provides the basis for the management of security risks of a health IT system. Security engineering is the analysis of whether a system provides adequate confidentiality, integrity, and availability to be acceptable for use. Security can interact with quality, safety, and usability in various ways, and the organization needs to balance these qualities to achieve a well-engineered system.

B.2.2 Security-related risk management process

The security process for an organization should use a risk-based management approach. Because attackers’ capabilities and motivations can evolve, security requires a separate risk management process from the one used to manage safety risk. Security risks that impact safety should also be assessed with the safety risk management process to ensure all sources of potential harm are managed in a comprehensive way. Developers should convene a dedicated, multidisciplinary team to consider, eliminate, or mitigate sources of security-related risk.

B.2.3 Use a systems approach

In evaluating the security of a health IT system, the techniques from systems engineering are utilized to examine all of the components, their interactions, and how the system interacts with the broader environment. Attackers can come from outside the system (via the internet) or may be inside the organization, either a disgruntled employee, or simply a user who makes a security error. NIST’s Special Publication 800-160, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems,* provides excellent guidance for application systems engineering to the security domain.

B.2.4 Full life cycle management

Security impacts the full life cycle of a health IT system and should begin when the system is initially being conceived, throughout all phases of design, during operations and through system retirement. As threats are constantly evolving, and vulnerabilities discovered in third-party code, the organization should plan for regular security updates throughout the operational phase of the system. When a system is retired, plans must be in place to eliminate any sensitive information in the system.

B.2.5 Focusing on *Integrity* and *Availability*

Security in healthcare is often viewed as a data confidentiality/privacy issue. However, health IT systems that are used to provide information to support patient diagnosis may have specific integrity and availability requirements. Inaccurate or inaccessible information may lead to incorrect care decisions and patient harm. User confusion or the inability to use a system due to poorly designed security controls can also be a source of reduced information availability.

B.2.6 Weakest link

Organizations should identify weak links in their system (which are often the people who are users of the system). Phishing and spear-phishing attacks can trick a user to accidentally do an attacker's bidding. Organizations should consider mechanisms to monitor system usage and train users who may put the system at risk. This should include audit mechanisms, so users understand that their actions can be analyzed, which can reduce the attractiveness of inappropriate behavior by malicious or careless insiders.

B.2.7 Defense in depth

Organizations should use a "defense in depth" strategy for securing a HIT system. No critical set of information should be protected by only a single control. An attacker should have to cross several layers of defenses in order to gain access to that information, modify it, or prevent others from accessing it.

B.2.8 Security testing

Developers should plan for and execute testing that specifically focuses on the security features of the system. Requirements-based testing primarily scrutinizes the "shalls," but exploitable vulnerabilities are often in the "shall nots." Security testing usually includes robustness testing, (i.e., "fuzz" testing and penetration testing). Robustness testing looks at how the system responds to malformed inputs. Penetration testing is done with a "white hat" hacker using the latest techniques to see if they can penetrate the system. Such experts can be within an organization or contracted out for specific skill sets not available internally. Because attacker's skills keep improving, the organization should plan for periodic penetration testing during the operational life of the system.

B.2.9 Proactive monitoring

With attackers' skills changing, and with new vulnerabilities being discovered in long-fielded software, the organization needs to proactively monitor the health IT system. This includes monitoring national databases and updates from key software suppliers. It also includes monitoring an operational system with tools such as intrusion detection systems, as well as security information and event management systems. It is also important that the information collected by such monitors be actively reviewed by the operations staff.

B.3 Security management resources

a) **AAMI TIR 57:2016/(R)2019**, *Principles for medical device security – Risk management.* Association for the Advancement of Medical Instrumentation; 2016. Arlington, VA.

b) **AAMI/IEC TIR80001-2-2:2012**, *Application of risk management for IT Networks incorporating medical device – Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks, and controls*. International Electrotechnical Commission; 2012. Geneva, Switzerland.

c) **AAMI/IEC TIR80001-2-8:2016**, *Application of risk management for IT Networks incorporating medical device – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2*. International Electrotechnical Commission; 2016. Geneva, Switzerland.

d) **IEC TR80001-2-9:2017,** *Application of risk management for IT Networks incorporating medical device – Part 2-9: Application guidance – Guidance for use of security assurance cases to demonstrate confidence in IEC/TR 80001-2-2 security capabilities*. International Electrotechnical Commission;2017. Geneva, Switzerland.

e) **ISO 27799:2016**, *Health informatics – Information security management in* health *using ISO/IEC 27002.* International Organization for Standardization; 2016, Geneva, Switzerland.

f) **IEC 62443-1-1:2009**, *Industrial communication networks - Network and system security – Part 1-1: Terminology, concepts, and models*. International Electrotechnical Commission; 2009. Geneva, Switzerland.

g) **IEC 62443-2-1:2010**, *Industrial communication networks – Network and system security: Part 2-1: Establishing an industrial automation and control system security program*. International Electrotechnical Commission; 2010. Geneva, Switzerland.

h) **IEC 62443-3-3:2013**, *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*, International Electrotechnical Commission; 2013. Geneva, Switzerland.

i) **ISO/IEC 15408-2:2008**, *Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components.* International Electrotechnical Commission; 2008. Geneva, Switzerland.

j) **ISO/IEC 15408-3:2008**, *Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components*. International Electrotechnical Commission; 2008. Geneva, Switzerland.

k) **ISO/IEC 27002:2013**, I*nformation technology – Security techniques – Code of practice for information security controls*. International Electrotechnical Commission; 2013. Geneva, Switzerland.

l) **NIST Special Publication 800-160**. *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.* National Institute for Standards and technology. Gaithersburg, MD.

m) **NIST Special Publication 800-53**. *Security and Privacy Controls for Federal Information Systems and Organizations.* National Institute for Standards and technology. Gaithersburg, MD.

Bibliography and cited references

Note: For more references and resources relating to Security Management, see B.3.

I. Standards

AAMI HIT1000-2 (in development), *Safety and effectiveness of health IT software and systems – Part 2: Application of quality systems principles and practices.* Association for the Advancement of Medical Instrumentation. Arlington, VA.

AAMI (PS)HIT1000-3:2019*Safety and effectiveness of health IT software and systems – Part 3: Application of risk management.* Association for the Advancement of Medical Instrumentation. Arlington, VA.

AAMI (PS)HIT1000-4: 2020, *Safety and effectiveness of health IT software and systems – Part 4: Application of human factors engineering.* Association for the Advancement of Medical Instrumentation. Arlington, VA.

ANSI/AAMI HE75:2009/(R)2013, *Human factors engineering – Design of medical devices.* Association for the Advancement of Medical Instrumentation; 2013. Arlington, VA.

ANSI/AAMI/IEC 62366-1:2015, *Medical devices – Part 1: Application of usability engineering to medical devices*. Association for the Advancement of Medical Instrumentation; 2015. Arlington, VA.

ANSI/AAMI/ISO 14971:2007, *Medical devices — Application of risk management to medical devices.* International Organization for Standardization; 2007. Geneva, Switzerland.

ANSI/AAMI/ISO 13485:2016, *Medical devices – Quality management systems — Requirements for regulatory purposes.* International Organization for Standardization; 2016. Geneva, Switzerland.

ANSI/AAMI/IEC TIR 80001-1:2010, *Application of risk* management for IT Networks incorporating medical devices. Association for the Advancement of Medical Instrumentation; 2010. Arlington, VA

ANSI/HFES 100:2007. *Human factors engineering of computer workstations*. Santa Monica, CA: Human Factors and Ergonomics Society; 2007.

ISO 9001:2015, *Quality management systems – Requirements.* International Organization for Standardization; 2015. Geneva, Switzerland.

ISO 9241-11:2018. *Ergonomics of human-system interaction – Part 11: Usability: Definitions and concepts*. International Organization for Standardization; 2018. Geneva, Switzerland.

ISO 31000:2018. *Risk management – Principles and guidelines.* International Organization for Standardization; 2009. Geneva, Switzerland.

ISO/IEC 15026-1:2013, Systems and software engineering – Systems and software assurance – Part 1: Concepts and vocabulary. . International Organization for Standardization; 2013. Geneva, Switzerland.

ISO 81001-1:202X: *Health informatics – Health software and health IT systems safety, effectiveness and security – Part 1: General principles and concepts.* International Organization for Standardization; 202x. Geneva, Switzerland.

II. Guides

ISO Guide 63:2012, *Guide to the development and inclusion of safety aspects in International Standards for medical devices.* International Organization for Standardization; 2012. Geneva, Switzerland.

ISO Guide 73:2009, *Risk management – Vocabulary.* International Organization for Standardization, Geneva. International Organization for Standardization; 2009. Geneva, Switzerland.

SAFER GUIDES https://www.healthit.gov/topic/safety/safer-guides

WHO 2011 Multi-professional Patient Safety Curriculum Guide. World Health Organization; 2011. Geneva, Switzerland.

III. Reports

Bipartisan Policy Center. An Oversight Framework for Assuring Patient Safety in Health Information Technology; 2013.

FDASIA Health IT Report: Proposed Strategy and Recommendations for a Risk-Based Framework. Jointly released by the Office of the National Coordinator for Health IT (ONC), the Food and Drug Administration (FDA), and the Federal Communication Commission (FCC); April 2014.

Health Care Industry Cybersecurity Task Force. *Report on Improving Cybersecurity in the Health Care Industry*.

Institute of Medicine (IOM). *Health* IT and Patient Safety: Building Safer Systems for Better Care. Washington DC: The National Academies Press; 2012.

Report of the ISO/TC 215-IEC/SC 62 Joint Task Force on Health Software (unpublished—available from International Organization for Standardization ISO/TC 215 or IEC/SC 62A. Geneva, Switzerland).

IV. Articles

Brown MJ, Shaw NT, Mador RL. *Mapping the sociotechnical healthcare ecosystem: Expanding the horizons of sociotechnical inquiry*. AMIA Annual Symposium Proceedings. 2008 Nov 6:1233-5.

Koppel R, Metlay, JP, Cohen A, Abaluck B, Locali A R, Kimmel SE, Strom BL. Role of computerized physician order entry systems in facilitating medication errors. *Journal of the American Medical Association.* 2005; 293(10): 1197-1203.

Lowry, SZ, Quinn MT, Ramaiah M, Schumacher RM, Patterson ES, North R, Abbott P. NIST 7804*: Technical evaluation, testing, and validation of the usability of electronic health records*. National Institute of Standards and Technology; 2012. Gaithersburg, Maryland.

Lowry SZ, Ramaiah M, Taylor S, Patterson E, Prettyman SS, Simmons D, Gibbons MC. *NISTIR 7804-1: Technical evaluation, testing, and validation of the usability of electronic health records: Empirically based use cases for validating safety-enhanced usability and guidelines for standardization.* National Institute of Standards and Technology; 2015. Gaithersburg, Maryland.

Ratwani RM, Fairbanks RJ, Hettinger AZ, Benda NC. Electronic health record usability: Analysis of the user-centered design processes of eleven electronic health record vendors. *Journal of the American Medical Informatics Association*. 2015.

Sittig DF, Singh H. A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. *BMJ Quality & Safety*. 2010;19:i68-i74.

Wiklund ME, Kendler J, Hochberg L, Weinger MB. *NIST GCR 15-996: Technical Basis for User Interface Design of Health IT*. National Institute of Standards and Technology; 2015. Gaithersburg, Maryland

Zhang J, Walji MF. TURF: Toward a unified framework of EHR usability. *Journal of Biomedical Informatics.* 2011:1056-1067.

V. Laws and Regulations

European Union. *Regulation 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices*

European Union. *Regulation 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices*

United States, *21st Century Cures Act*, Public Law 114–255—Dec. 13, 2016

United States, *2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications,* Health and Human Services Department, Final Rule, Oct 6, 2015