Health IT Software and Systems – Part 1: Fundamental concepts and principles

Association for the Advancement of Medical Instrumentation

This is a working draft of AAMI HIT1000-1.

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

Keywords:

American National Standard
Health IT Software and Systems – Part 1: Fundamental concepts and principles

WD stage

Warning for WDs and CDs

This document is not a standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as a standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

MEMBERS OF THE AAMI HEALTH IT COMMITTEE AND AFFILIATED WORKING GROUPS ARE REQUESTED TO SUBMIT COMMENTS ON THIS DRAFT TO jlewelling@aami.org BY NOON, FRIDAY 20 JANUARY 2017.

A WORD COMMENT FORM HAS BEEN PROVIDED VIA AAMI COMMITTEE CENTRAL TO USE IN PROVIDING COMMENTS.

Contents

Foreword ......................................................................................................................................................................................... 7

Introduction......................................................................................................................................................................................... 8

1 Scope ............................................................................................................................................................................................. 10

2 Normative definitions [To be added] ........................................................................................................................................... 10

3 Terms and definitions [Additional terms to be added] ........................................................................................................... 11

4 Context and concepts ............................................................................................................................................................... 13

  4.1 HIT in a complex adaptive sociotechnical eco-system ........................................................................................................ 13
  4.2 Health IT life cycles ................................................................................................................................................................. 15
  4.3 Patient Safety in HIT software and systems ......................................................................................................................... 15
  4.4 Quality management in health IT software and HIT systems ................................................................................................. 15
  4.5 Risk management of safety in health IT software and HIT systems ..................................................................................... 16
  4.6 Usability in HIT software and systems .................................................................................................................................. 16
  4.7 Shared responsibility ............................................................................................................................................................... 18
  4.8 Roles and responsibilities ........................................................................................................................................................ 18
  4.9 HIT software life cycle ........................................................................................................................................................... 20
  4.10 Transition points ................................................................................................................................................................. 20
  4.11 Health Software Life Cycle Stages and activities .............................................................................................................. 21
  4.12 Views across the health software life cycle by role ........................................................................................................... 26
  4.13 Applying quality and risk management to existing systems ............................................................................................... 27
  4.14 HIT system risk benefit analysis .......................................................................................................................................... 27

5 Principles .................................................................................................................................................................................... 27

  5.1 Quality management principles ............................................................................................................................................. 27
      5.1.1 General ................................................................................................................................................................................. 27
      5.1.2 Customer and Stakeholder Focus .................................................................................................................................. 28
      5.1.3 Leadership ........................................................................................................................................................................ 28
      5.1.4 Engagement of People .................................................................................................................................................... 28
      5.1.5 Process Approach ........................................................................................................................................................ 28
      5.1.6 Improvement ................................................................................................................................................................. 28
5.1.7 Evidence-based Decision Making ................................................................. 29
5.1.8 Relationship management ............................................................................. 29
5.2 Risk management principles ........................................................................... 29
  5.2.1 General .......................................................................................................... 29
  5.2.2 Value creation and protection ...................................................................... 29
  5.2.3 Integration ...................................................................................................... 29
  5.2.4 Structured approach ...................................................................................... 30
  5.2.5 Customized .................................................................................................... 30
  5.2.6 Inclusive ........................................................................................................ 30
  5.2.7 Dynamic and responsive ............................................................................. 30
  5.2.8 Best available information .......................................................................... 30
  5.2.9 Human and cultural factors ......................................................................... 30
  5.2.10 Continual improvement ............................................................................. 30
5.3 Usability engineering principles ...................................................................... 31

6 General requirements for health IT ................................................................ 31
  6.1 Application ........................................................................................................ 31
  6.2 Health IT quality system general requirements ............................................. 31
  6.3 Health IT processes .......................................................................................... 31
  6.4 Competences of personnel ............................................................................ 31
  6.5 Top Management responsibilities ................................................................. 31
  6.6 HIT Safety Officer .......................................................................................... 31
  6.7 Non-health products and COTS products ..................................................... 32
  6.8 Regular process review ................................................................................... 32
  6.9 Incident Management and Reporting ............................................................ 32

7 Documenting HIT safety .................................................................................. 32

Annex A (informative) ANNEXES TO BE ADDED AS NEEDED. ......................... 34
  A.1 Clause ............................................................................................................. 34
  Bibliography TBD ................................................................................................. 34
Foreword

Suggestions for improving this recommended practice are invited. Comments and suggested revisions should be sent to Technical Programs, AAMI, 4301 N. Fairfax Drive, Suite 301, Arlington, VA 22203-1633.

NOTE—This foreword does not contain provisions of the AAMI xx, title (AAMI xx:xxx), but it does provide important information about the development and intended use of the document.
**Introduction**

**Application of Quality Principles and Risk Management Processes Across the Health IT Lifecycle**

There is growing recognition of the vital role sector-specific health information technology (IT) safety management standards can play in enhancing health IT safety and quality. In the United States, the April 2014 FDASIA Health IT Report: Proposed Strategy and Recommendations for a Risk-Based Framework, identified the development and application of standards and best practices, specifically in the areas of quality systems, risk management and usability as core priorities and the preferred way to support health IT innovation and patient safety. The FDASIA Report identified the risks to patient safety from “health management health IT” and, to a lesser degree, “administrative health IT,” as best addressed through a private sector, standards-based framework, without need for the higher level of regulation of “medical device health IT”. The FDASIA Report built upon work by other prestigious organizations, that advocated adherence to standards and best practices as a framework for shared responsibility for health IT safety throughout the health IT product lifecycle. This approach has received widespread support from private sector groups whose participation in and support of next steps to build this framework is crucial for its success. This triad—of quality systems, risk management, and user-centered design—is already used successfully to advance a culture of safety in many high-risk industries like medical devices, nuclear engineering, and aeronautics.

Internationally, the need for health-IT specific quality systems, risk management, and usability standards has been recognized by an ad hoc task group on health software, operating under the joint auspices of the ISO/TC 215, Health informatics, and IEC/SC 62A, Common aspects of electrical equipment used in medical practice. While standards designed specifically for the health IT sector must be consistent with general international quality system and risk management standards, the general standards, which apply to a broad range of technologies and medical devices, have proven inadequate for the complex, adaptive nature of health IT. General standards do not incorporate an understanding of the health IT product lifecycle or of the sociotechnical context in which shared responsibility by many different organizations and individuals is vital -- technology developers, clinicians, the people and organizations that implement and maintain health IT, risk management organizations, private and public sector oversight bodies, and others. Shared standards, which identify roles and responsibilities specific to health IT quality management and risk management processes, create a common framework for many different organizations and individuals to work both independently and cooperatively to ensure and foster the safety, safe use, and continuous improvement of health IT. Health IT sector-specific standards are needed to ensure needed innovation and to accommodate rapid timeframes for safety enhancements and fixes, as well as for continuous improvement. Health IT specific standards could help clarify processes that meet ONC’s certification criteria for EHR technology.

For those reasons, there is a need for standards specifically applicable to health IT for quality management and risk management. The AAMI/HIT1000 series is intended fulfil this need. The AAMI/HIT1000 series will apply to health IT, throughout the health IT lifecycle. These standards will not supplant existing quality management systems or risk management frameworks, but will facilitate shared responsibility among the many organizations and individuals that develop, implement, and use health IT by identifying specific roles, defining responsibilities needed to ensure health IT safety and quality, and creating a common framework for cooperation and collaboration to address risks.

The AAMI/HIT 1000 series is envisioned as comprising the following parts:
• HIT1000-1, Health IT software and systems — Part 1: Fundamental concepts and principles
• HIT1000-2, Health IT software and systems — Part 2: Application of quality systems principles and practices
• HIT1000-3, Health IT software and systems — Part 3: Application of risk management
• HIT1000-4, Health IT software and systems — Part 4: Application of human factors engineering

This part of the series, HIT1000-1, identifies the fundamental concepts and principles needed to maintain safe, secure and effective HIT software and systems.


AAMI HIT1000-1 - Health IT Software and HIT Systems – Part 1: Fundamental concepts and principles

1 Scope

1.1 This part of AAMI HIT1000 (Part 1: Fundamental concepts and principles) identifies the fundamental concepts and principles needed to maintain safe, secure and effective HIT software and HIT systems.

1.2 This standard identifies the roles, and defines the responsibilities, activities and best practices that are necessary for managing safety, security and effectiveness of HIT software and HIT systems. It applies to all sizes and types of health service delivery organizations and to HIT vendors developing, implementing and using HIT software and HIT systems within their sociotechnical use context.

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

1.4 It defines the points in the life cycle where different roles assume primary responsibility for maintaining safety, security and effectiveness, and identifies the communication necessary between 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 lifecycle. At those stages, the HDO would also be serving as a developer and would assume the appropriate responsibilities of that role.

1.5 This standard provides guidance for HIT software and HIT Systems

2 Normative definitions [To be added]

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.
3 Terms and definitions [Additional terms to be added]

3.1 Health IT (HIT)
application of information processing involving both computer hardware and software that deals with the storage, retrieval, sharing, and use of health care information, data, and knowledge for communication and decision making.

[SOURCE: https://www.healthit.gov/unintended-consequences/content/glossary.html#h]

3.2 Health IT software (HIT software)
software that is intended to store, retrieve, share, and use health care information, data, and knowledge for communication and decision making.

Note 1: Health software consists of many components including programs, executable code, libraries, value sets, algorithms, libraries 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 software may be incorporated into an HIT system, or may be an independent part of the technology element of the healthcare sociotechnical eco-system if it is not integrated with other components.

3.3 Health IT system (HIT system)
Integrated combination of interacting hardware and health software, data, and supporting health IT infrastructure and services that is configured and integrated to support specific health care business processes and objectives for a health care delivery organization.

Note 1: This typically entails the integration of multiple software components through interfaces to capture, communicate and process information, supported by an organization’s IT infrastructure.

Note 2: An organization’s IT infrastructure may support multiple HIT systems.

3.4 Healthcare sociotechnical eco-system
The people, process (workflow), technology, organization, and external environment organized to deliver services for healthcare or wellbeing.

Note 1: The interaction and interdependence of the elements of the healthcare sociotechnical eco-system with each other is significant since safety is an emergent property of the sociotechnical eco-system.

Note 2: HIT systems are a key part of the technology that enables the delivery of healthcare or wellbeing.

3.5 Patient Safety
The prevention and mitigation of harm caused by errors of omission or commission that are associated with healthcare, and involving the establishment of operational systems and processes that minimize the likelihood of errors and maximize the likelihood of intercepting them when they occur.

[SOURCE: National Quality Forum]
3.6 Risk

effect of uncertainty
Note 1 to entry: An effect is a deviation from the expected — positive or negative.
Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.
Note 3 to entry: Risk is often characterized by reference to potential events (as defined in ISO Guide 73:2009, 3.5.1.3) and consequences (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these.
Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.
Note 5 to entry: The word “risk” is sometimes used when there is the possibility of only negative consequences.
Note 6 to entry: This constitutes one of the common terms and core definitions for ISO management system standards given in Annex SL of the Consolidated ISO Supplement to the ISO/IEC Directives, Part 1. The original definition has been modified by adding Note 5 to entry.

3.7 Risk management

coordinated activities to direct and control an organization with regard to risk (1.1)

[SOURCE: ISO Guide 73]

3.8 Stakeholder

person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity
Note 1 to entry: A decision maker can be a stakeholder.

[SOURCE: ISO Guide 73]

3.9 Transition Points

Points in the health software and HIT system lifecycle where the primary responsibility for patient safety moves (transitions) from one role (and in some cases from one organization) to another.
4 Context and concepts

4.1 HIT in a complex adaptive sociotechnical eco-system

Health information technology exists as part of a larger sociotechnical multi-disciplinary system that we call the healthcare sociotechnical eco-system. This sociotechnical eco-system includes technology, process (workflow), people, organization and external environment. HIT software exists as part of the technology component of this sociotechnical eco-system. It may be incorporated into an HIT system which may contain other HIT software and IT infrastructure. HIT software, HIT systems and other supporting infrastructure such as databases, servers, data centers, etc. are all part of the technology component of the healthcare sociotechnical eco-system as shown in the figure below.
This sociotechnical eco-system has been described as a complex adaptive system. Because it is an adaptive system, it is constantly changing; evolving to address changes in people, workflow, organization, external environment or technology. When a safety issue is identified these adaptations might be workarounds by clinicians, software changes by developers, staffing changes by the organizations such as adding personnel in a certain area, or technology changes by IT operators such as changing a firewall, modifications to system interfaces or adding a wireless access point. We want the eco-system to adapt to address the safety issue of course, but an adaptation that addresses the root cause and does not result in some new safety issue would be the preferable course of action.
4.2 Health IT life cycles

Any individually identifiable software product intended for healthcare or wellbeing is part of the technology component of the healthcare eco-system. Health IT software can also be a component of a larger health IT system. The health IT software could 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 this health software is like a living organism; it is conceived, brought into existence, matures and eventually dies. We can identify major stages of the life 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 as a result of actions using processes for their performance.

HIT systems are composed of integrated components assembled for a specified healthcare purpose. These systems also have their own life cycle[s].

The analogy with a living organism does not hold for the sociotechnical environment. A more apt analogy for these environments would be an eco-system, where many types of organisms exist in complex and dynamic relationships. Such an environment evolves and changes over time, but it cannot be said to mature and does not reach an end of life point. In this environment, there are not life cycle stage changes for the entire environment, but changes in the relationships as individual components including HIT systems move through their life cycle.

4.3 Patient Safety in HIT software and systems

There are two aspects of patient safety. The first aspect is to reliably perform the processes and activities necessary for safely providing the benefits of HIT for patients. This aspect is addressed by the discipline of HIT quality system management.

The second is to prevent the HIT system from causing harm to patients, including harm caused by not making the benefits of the HIT available to patients by inadvertently introducing barriers to adopting beneficial HIT. This is addressed by the discipline of HIT risk management.

Usability plays a key role in both aspects of patient safety.

4.4 Quality management in health IT software and HIT systems

The intent of quality management is to assess the manner in which a system satisfies the stated and implied needs of various stakeholders. Ultimately, a quality management system addresses aspect of value provided to the organization. In this series of standards the objective is patient safety. Quality management is used to manage the extent to which a system needs to be effective, efficient, satisfying to use, and free of defects.

Quality management for patient safety (hereafter referred to as quality management) is a process to which a product or system can be used by specific users to meet their needs to achieve specific goals with effectiveness, efficiency, freedom from risk and satisfaction in specific contexts of use. While managing quality for health software is necessary, when that health software is part of an HIT system which is part of a larger sociotechnical eco-system, quality management of the health software is not sufficient to achieve
patient safety. In these complex systems patient safety cannot be achieved just by managing the quality of
the individual components of the system (e.g. the health software).

It is essential for these complex systems that the expectations of all parties with a stake in the system are
aligned with the actual functioning of the system. This allows consideration of all quality concepts to be
made when a party believes a change or adaptation is necessary. The goal of quality management is to
meeting the customers’ and organization’s requirements. This is true whether the change is within the HIT
system or in the context in which the HIT system is used, (e.g. user interaction, workarounds, work flow).

Given the inter-relationships between components, and the need to manage quality should include
alignment of testing & validation assessment processes to share insights and optimize synergies.

4.5 Risk management of safety in health IT software and HIT systems

The intent of risk management is to manage the effect of uncertainty on achieving objectives. In this series
of standards the objective is patient safety. Risk management is used to manage the effect of health IT
uncertainty to prevent an unacceptable risk of patient harm. What is an unacceptable risk of patient harm
is determined by each organization based on its risk appetite, the amount and type of risk that is acceptable
to the organization.

Risk management for patient safety (hereafter referred to as risk management) is a process that is used to
minimize the uncertainty of how health IT affects patient safety during each stage of the HIT software and
system life cycle. Risk management asks the questions: “What can go wrong?”; “What can you do?”; “Did it
work?”; “Is it enough?”

While managing patient safety risks due to health software is necessary, when that health software is part
of an HIT system which is part of a larger sociotechnical system, risk management of the health software is
not sufficient to achieve patient safety. In these complex systems patient safety cannot be achieved just by
managing the risk to patient safety of the components of the system (e.g. the health software). It is essential
for these complex systems that the expectations of all parties with a stake in the system are aligned with
the actual functioning of the system. This allows consideration of all risks to be made when a party believes
a change or adaptation is necessary. The goal of risk management is to proactively recognize how patient
harm could occur and then reduce the risk of it occurring to an acceptable level by controlling the health IT
effects that could result in that harm. This is true whether the change is within the HIT system or in the
context in which the HIT system is used, (e.g. user interaction, workarounds, work flow).

Given the inter-relationships between safety, security and privacy, and the need to manage risks in all three
areas, organizations should align their risks assessment processes in all three areas to share insights and
optimize synergies.

4.6 Usability in HIT software and systems

The ability to deliver high quality health care is closely tied to the quality of an HIT system's user interface
design and its resulting usability (with a particular focus on use-safety). Simply stated, a poorly designed
HIT system can induce use errors that lead to patient injury and even death. Therefore, as HIT systems
become increasingly integral to healthcare delivery, it will become ever more important to minimize the
chance of potentially harmful use errors during their use.
Mirroring the well-established approach to reducing risk that prevails in other industries (e.g., power generation, aviation, transportation, medical devices) where use errors can lead to injury to the user, developers should follow a user interface design process that seeks to identify potentially harmful use errors and decrease their likelihood of occurrence. Fortunately, a use-safety focused design process typically also increases task effectiveness, work efficiency, and user satisfaction. Moreover, efforts to optimize an HIT system's user interface design are closely aligned with the broad-based goal of ensuring patient safety by means of comprehensive risk management.

In addition to use-safety and effectiveness, another key component of an optimal user experience is usability, especially as it relates to user satisfaction. Satisfaction with a technology or software application influences users’ willingness to use the product and, when they do, to tolerate aspects of the user interface that do not fully meet their needs. User satisfaction is usually influenced by multiple, interrelated user interface design features, rather than just one or a few features. For example, a user might be satisfied by an HIT system that has the following characteristics:

- Intuitiveness enabling the user to perform basic tasks without first reading instructional materials.
- Workflow that closely matches the conventional clinical workflow that existed before HIT system implementation.
- Visual appeal resulting from the balanced-looking arrangement of onscreen contents, the use of harmonious colors, easy to interpret icons augmented by text labels, large and three-dimensional looking controls (i.e., buttons), and the use of blank space to separate blocks of information.

Note that these characteristics could have a positive influence on HIT use-safety and effectiveness. But, even if they do not, a well-designed HIT system should possess these and/or comparable interface characteristics to foster task efficiency and user satisfaction.

Accordingly, developers should consider taking the following steps to increase an HIT system’s usability:

- Address usability concerns along with use-safety and effectiveness concerns during user research activities.
- Write usability-focused user interface requirements.
- Conduct benchmarking studies of competitor systems to better understand user expectations, prominent design trends, and opportunities for market differentiation through usability improvements.
- Establish quantitative usability goals that will be upheld with the same diligence as other technical or software engineering goals (e.g., software response time).
- Invest user interface design effort into making the system visually appealing and intuitive to use.

---

• Conduct a variety of usability-related evaluations, such as expert reviews and usability tests.

• Iterate the design process (i.e., establish user interface requirements → design → model → test) to the extent necessary to ensure usability.

Developers are likely to find that usability is often a natural by-product of efforts to ensure an system’s use-safety and effectiveness because an investment in user-centered design can have a positive influence on all three factors. However, developers might have to invest at least some extra effort to ensure an HIT system’s usability, which should pay off well in terms of higher user satisfaction.

4.7 Shared responsibility

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

4.8 Roles and responsibilities

Roles are not specific to organizations. Hospitals can act as developers and software companies can be implementers or operators. An individual can have more than one role. Within a role many functions may be performed. These functions may be performed by one or many individuals.
### Table 1—Roles and associated responsibilities

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Top Management</strong></td>
<td>Group of people who direct and control an organization and have overall accountability for a Health IT System.</td>
</tr>
<tr>
<td><strong>HIT Safety Officer</strong></td>
<td>Person in an organization responsible for ensuring the safety of a Health IT System in that organization.</td>
</tr>
<tr>
<td><strong>Primary Safety Owner</strong></td>
<td>The role that has the primary responsibility for patient safety during a life cycle stage.</td>
</tr>
<tr>
<td><strong>Primary Quality Owner</strong></td>
<td>The role that has primary responsibility for quality management during a life cycle stage.</td>
</tr>
<tr>
<td><strong>Primary Risk Owner</strong></td>
<td>The role that has primary responsibility for risk management during a life cycle stage.</td>
</tr>
<tr>
<td><strong>Primary Usability Owner</strong></td>
<td>The role that has primary responsibility for usability during a life cycle stage (with a particular focus on use-safety).</td>
</tr>
<tr>
<td><strong>Developer</strong></td>
<td>Role responsible for the design, development, manufacture and maintenance of the health software (also referred to as “manufacturer” or “supplier” in some standards)</td>
</tr>
<tr>
<td><strong>Integrator</strong></td>
<td>Role responsible for the technical installation, configuration and integration of HIT software with the other technology being used by the healthcare organization.</td>
</tr>
<tr>
<td><strong>Implementer</strong></td>
<td>Role responsible for the clinical installation and integration of the HIT software in the clinical setting (an implementer may be the developer or the owner).</td>
</tr>
<tr>
<td><strong>Business Owner</strong></td>
<td>The healthcare organization procuring the software and accountable for the overall safety, security and effectiveness of the healthcare sociotechnical eco-system.</td>
</tr>
<tr>
<td><strong>Operator</strong></td>
<td>Role responsible for keeping the HIT system operational (and/or may be the implementers for a managed service).</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>Persons using the health software in the clinical setting, which may include, for example, consumers in the case of personal health records.</td>
</tr>
</tbody>
</table>
4.9 HIT software life cycle

Figure 2 - Health software life cycle within an HIT system. Iteration and recursion possible on all paths

Figure 2 shows the stages of the life cycle of a health software component as it is developed, integrated into an HIT system, implemented in a sociotechnical eco-system and used in a clinical context until it is decommissioned and retired. At each stage actions need to be taken to protect patient safety.

4.10 Transition points

As the health software (or HIT system that incorporates the health 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 transferred to the role assuming the primary responsibility. 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.
NOTE The health software lifecycle stages, while identified linearly on the figure above, do include a complex array of linear and iterative actions to provide the continuous management of that software by all parties involved.

4.11 Health Software Life Cycle Stages and activities

A draft life cycle is listed below. It should be noted that the stages and activities may be iterative and are not necessarily sequential. In most cases many activities may occur concurrently, but they will complete sequentially.
<table>
<thead>
<tr>
<th>Lifecycle Stage</th>
<th>Lifecycle steps</th>
<th>Step Definition and activities needed for patient safety during the step</th>
<th>Role(s) involved in safety management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design/Develop</td>
<td>Design and development is a process (or a set of processes) using resources to transform requirements (inputs) into characteristics or specifications (outputs) for products, processes and systems.</td>
<td>The primary safety owner during the design and development stage is the developer.</td>
<td></td>
</tr>
<tr>
<td>Concept/requirements</td>
<td>Conceiving, imagining and specifying the initial design of the aesthetics and primary functions of the software.</td>
<td>Developer, User</td>
<td></td>
</tr>
<tr>
<td>Task Analysis</td>
<td>A 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 activity.</td>
<td>Developer, Primary Usability Owner, Primary Risk Owner</td>
<td></td>
</tr>
<tr>
<td>Design/Development</td>
<td>A design is concerned with how the problem is to be resolved.</td>
<td>Developer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The design is transformed into a product, process or system.</td>
<td>Developer</td>
<td></td>
</tr>
<tr>
<td>Formative Evaluation</td>
<td>Conduct formative usability evaluations throughout the development process, and use the results to improve the system’s design/efficacy.</td>
<td>Developer, Primary Safety Owner, Primary Quality Owner, Primary Usability Owner</td>
<td></td>
</tr>
<tr>
<td>Verification</td>
<td>The output of the development step is reviewed, inspected or tested to establish and document that it correctly implements the requirements.</td>
<td>Developer</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>Summative Evaluation</td>
<td>Conduct summative evaluations on the product-equivalent system.</td>
<td>Developer, Primary Safety Owner, Primary Quality Owner, Primary Usability Owner</td>
<td></td>
</tr>
<tr>
<td>Delivery</td>
<td>A release is a specific version of a product, service or system that is released for a particular purpose and made available by distribution to owners or implementers.</td>
<td>Developer, Business owner, Implementer</td>
<td></td>
</tr>
</tbody>
</table>

**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 software meets the organizations needs and that it can be used safely in the business owner’s healthcare sociotechnical eco-system. It is the business owner’s responsibility to make the correct determination.

| 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. | The primary safety owner during the acquisition is the business owner Business owner. |

**Transition point from Business owner to Integrator**

At this transition, the HIT owner provides the planned context of use of the HIT software in the HIT system and healthcare sociotechnical eco-system; and any known configuration or customization of the HIT software, training of operators or users, or special testing and monitoring of the integrated HIT system to the integrator.
<table>
<thead>
<tr>
<th>Integration</th>
<th>Installation</th>
<th>Software conformance testing and certification may also be included in the implementation step, either as a first or pre-installation step.</th>
<th>The primary safety owner during integration is the integrator. Integrator, Developer, Implementer, Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configuration</td>
<td></td>
<td>Integrator, Developer</td>
</tr>
<tr>
<td></td>
<td>Customization</td>
<td></td>
<td>Integrator, Developer</td>
</tr>
<tr>
<td></td>
<td>Integration</td>
<td></td>
<td>Integrator</td>
</tr>
<tr>
<td></td>
<td>Data sourcing and transformation</td>
<td></td>
<td>integrator</td>
</tr>
<tr>
<td></td>
<td>Integration Testing</td>
<td></td>
<td>integrator</td>
</tr>
</tbody>
</table>

**Transition point from Integrator to Implementer**

At this transition the integrator provides information about any hazards that were identified during integration, including those that may have emerged during configuration and customization. Assumptions, mitigation strategy, and evidence or logic for adequacy of mitigations are also provided. Any hazards that are expected to be mitigated during implementation are identified.
<table>
<thead>
<tr>
<th>Implementation</th>
<th>Workflow assessment and optimization</th>
<th>The primary safety owner during implementation is the Implementer. Roles having shared safety responsibility are: Implementer, user</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decision support</td>
<td>Implementer, user</td>
<td></td>
</tr>
<tr>
<td>Patient identification and data quality</td>
<td>Implementer, user</td>
<td></td>
</tr>
<tr>
<td>Change management and training</td>
<td>Implementer, user</td>
<td></td>
</tr>
<tr>
<td>Deployment</td>
<td>Implementer, user</td>
<td></td>
</tr>
<tr>
<td>Pilot or limited production roll-out</td>
<td>Implementer, user</td>
<td></td>
</tr>
<tr>
<td>Go-Live</td>
<td>To make some system, which had been under development or operating in a limited test mode, fully active so that its intended users can access it. Implementer, Operator, user</td>
<td></td>
</tr>
<tr>
<td>Go-Live</td>
<td>To make some system, which had been under development or operating in a limited test mode, fully active so that its intended users can access it. Implementer, Operator, user</td>
<td></td>
</tr>
</tbody>
</table>
**4.12 Views across the health software life cycle by role**

A view provides responsibilities of a particular role looking across all stages and steps of the health software life cycle. A view is associated with a role, for instance providing all the activities that are performed by a health software developer from concept to disposal of the health software.

<table>
<thead>
<tr>
<th>Operational Use in the clinical setting</th>
<th>Post-deployment monitoring</th>
<th>Monitoring and optimizing network, database, infrastructure support to the HIT system</th>
<th>The primary safety owner during operational use is the Operator. Roles sharing safety responsibility are: Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modification and maintenance</td>
<td>Health software support is the modification of health software or the HIT system after delivery to correct faults, improve technical performance or other attributes, or to add or improve functionality. Accuracy, timeliness, integrity, usable for purpose</td>
<td>Developer, Integrator, Operator, User</td>
<td></td>
</tr>
<tr>
<td>Disposal/ Decommission</td>
<td>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.</td>
<td>Operator, User,</td>
<td></td>
</tr>
</tbody>
</table>
4.13 Applying quality and risk management to existing systems

Just as risk management plans should be periodically reviewed and updated (especially when system changes occur), risk assessments 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 it.

4.14 HIT system risk benefit analysis

HIT system risk benefit analysis is used to justify the residual HIT system risk associated with a hazard once all practicable measures to reduce the HIT system risk have been applied. If, after applying these measures, the HIT system risk is still judged not acceptable, a clinical risk benefit analysis is needed to establish whether the HIT system is likely to provide more clinical benefit than harm.

The decision as to whether the residual HIT system risks associated with a hazard is outweighed by the benefits the HIT system provides is essentially a matter of judgement by experienced and knowledgeable individuals, which would normally include the HIT Safety Officer 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 HIT system risk benefit judgements have a responsibility to understand and take into account 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 an individual patient.

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

Proceeding with a deployment that retains unacceptable risk would need explicit approval by Top Management using established governance processes. In such a case, the HIT system risk would have to be communicated across the Health organization to ensure full awareness.

The HIT system risk benefit analysis needs to be documented in the HIT system Safety Case Report and whether the residual HIT system risk is now acceptable needs to be documented.

5 Principles

5.1 Quality management principles

5.1.1 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 developed and updated by international experts of ISO/TC 176, which is responsible for developing and
maintaining ISO's quality management standards. These QMPs can be used as a foundation to guide an organization's performance improvement and will be referenced throughout this document. 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 HIT software or an HIT System.

5.1.2 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 to as well as consume and share their health information.

5.1.3 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.

5.1.4 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.

5.1.5 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 achieve the organization’s quality objectives effectively and efficiently. Ensure the necessary information is available to operate and improve the processes and to monitor, analyse and evaluate the performance of the overall system. Manage risks that can affect outputs of the processes and overall outcomes of the quality management system.

5.1.6 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.
5.1.7 Evidence-based Decision Making

Decision making can be a complex process, and it always 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. This requires that the organization determine, measure and monitor key indicators to demonstrate the organization’s performance, ensuring that data and information are sufficiently accurate, reliable and secure. The required data should be available to the relevant people.

5.1.8 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. Organization 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 and other interested parties.

5.2 Risk management principles


5.2.1 General

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

5.2.2 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.

5.2.3 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.
5.2.4 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.

5.2.5 Customized

Risk management is 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.

5.2.6 Inclusive

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

5.2.7 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.

5.2.8 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 take into account any limitations and uncertainties of the data, modelling, and divergence among experts.

5.2.9 Human and cultural factors

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

5.2.10 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.
5.3 Usability engineering principles

The principles below summarize best practices for applying usability engineering to health IT system development and implementation. These principles are adapted from NIST GCR_15-996 – Technical Basis for User Interface Design of Health IT.

6 General requirements for health IT

6.1 Application

These requirements apply to every organization that is involved in developing, implementing and operating HIT software or an HIT system.

6.2 Health IT quality system general requirements

During each stage of the Health IT lifecycle a quality system that addresses relevant quality principles, shall be defined, documented and implemented by the quality system owners of the organizations involved in that stage.

6.3 Health IT processes

During each stage of the Health IT lifecycle quality and risk management processes shall be defined, documented and implemented by the Safety Officer of that stage.

6.4 Competences of personnel

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

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

6.5 Top Management responsibilities

6.5.1 In executing the HIT processes for a given life cycle stage, Top Management shall:

• make available sufficient resources
• assign competent personnel from each of the specialist areas that are involved in assuring the safety of the HIT Software or HIT System
• appoint an HIT Safety Officer.

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

6.6 HIT Safety Officer

6.6.1 An HIT Safety Officer shall be suitably qualified and have clinical knowledge.
6.6.2 An HIT Safety Officer shall be knowledgeable in quality and risk management and their application to HIT domains.

6.6.3 An HIT Safety Officer shall make sure that the processes defined for HIT are followed.

6.7 Non-health products and COTS products

Any non-health product or Commercial Off the Shelf (COTS) product that is included within HIT shall be assessed for quality and safety.

6.8 Regular process review

Each organization shall formally review its HIT processes at planned, regular intervals.

6.9 Incident Management and Reporting

Given the increasing complexity of HIT software and systems, incidents will occur and it is important that incidents (including near misses) are reported and managed through a pre-defined process so that the risk owner(s) can promptly investigate incidents and take any necessary corrective action to prevent further harm. Especially in those cases where there is a systemic fault, it is important that these incidents be communicated to all parties involved in a transparent way so that appropriate risk management action can be taken to reduce the likelihood of reoccurrence.

7 Documenting HIT safety

These requirements apply to every organization that is involved in developing, integrating, implementing and operating HIT software or an HIT System. Each stage (development, integration, implementation, operation) should have its own documentation that includes:

- decisions made that influence the HIT quality management and risk management activities;
- HIT Quality Management and Risk Management Plans, approved by the HIT Safety Officer;
- a record of hazards identified;
- an HIT safety case addressing the identified hazards;
- an HIT safety case report (when the Primary Risk Owner changes at a risk management transition point, an HIT Safety Case Report shall be provided to the successor Primary Risk Owner);
- safety Incident Management Records during the life cycle stage.

As the HIT software advances through its life cycle, its safety case is incorporated into the HIT system safety case and the safety case for using the HIT system in the larger HIT-enabled sociotechnical ecosystem. This is illustrated in the figure below.
Operational use in a clinical setting. Monitoring, event management, support

Figure 4 - Safety cases through the life cycle
Annex A (informative) ANNEXES TO BE ADDED AS NEEDED.

A.1 Clause

Type text here - use subclauses if required e.g. A.1.1 or A.1.1.1.

Bibliography TBD

[1] ISO ######-##:20##, General title — Part ##: Title of part