American National Standard

AAMI HIT1000-1 (PS):2018

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 a Provisional American National Standard on 5 October 2018 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, assurance case, health IT system, sociotechnical system

Provisional AAMI/American National Standard

A Provisional National Standard is a standard for trial use. It does not represent the same level of national consensus as a full American National Standard and has not been approved by ANSI. This Provisional National Standard must be advanced for approval as a full American National Standard within two years of its approval (5 October 2018).

The existence of any AAMI standard does not in any respect preclude anyone, whether they have approved the standard or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to that standard.

CAUTION NOTICE: This Provisional AAMI/American National Standard may be revised or withdrawn at any time. Interested parties may obtain current information on all AAMI standards by calling or writing AAMI, or by visiting the AAMI website at www.aami.org

All AAMI standards, recommended practices, technical information reports, provisional standards, and other types of technical documents developed by AAMI are *voluntary*, and their application is solely within the discretion and professional judgment of the user of the document. Occasionally, voluntary technical documents are adopted by government regulatory agencies or procurement authorities, in which case the adopting agency is responsible for enforcement of its rules and regulations.

Published by

For a complete copy of this AAMI document, contact AAMI at +1-877-249-8226 or visit www.aami.org.

AAMI
4301 N. Fairfax Drive, Suite 301
Arlington, VA 22203-1633
www.aami.org

Printed in the United States of America

ISBN 978-1-57020-706-8

Contents

Page

Committee representation ..... **iv**
Foreword ..... **vi**
Introduction ..... **vii**
1 Scope **1**
2 Terms and definitions **2**
3 Context and concepts **6**
3.1 Health IT in a complex adaptive sociotechnical ecosystem 6
3.2 Health IT lifecycles 6
3.3 Data management across the lifecycle 7
3.4 Patient safety and health IT software and systems 7
3.5 Quality management and health IT software and systems 7
3.6 Safety risk management in health IT software and systems 8
3.7 Usability in health IT software and systems and human factors engineering 8
3.8 Shared responsibility for safety 9
3.9 Health IT lifecycle roles and responsibilities 9
3.10 Health IT software lifecycle 10
3.11 Safety roles and responsibilities 11
3.12 Transition points 11
3.13 Activity views across the health IT software lifecycle by role 11
3.14 Applying essential health IT lifecycle processes to existing systems 11
3.15 Health IT system risk benefit analysis 11
3.16 Safety assurance case 12
4 Principles **13**
4.1 Quality management principles 13
4.2 Risk management principles 14
4.3 Human factors engineering principles 15
5 Fundamental requirements **16**
5.1 Application 16
5.2 Essential health IT lifecycle processes (quality, human factors, and risk) 17
5.3 Competencies of personnel 17
5.4 Top management responsibilities 17
5.5 Health IT safety owner 17
5.6 Products not intended for the purpose of affecting human health and health care 17
5.7 Monitoring, surveillance, reporting and management 17
6 Documenting health IT safety **18**
Annex A (normative)—Health IT software lifecycle stages and activities **20**
Annex B (informative)—Useful guidance on security management for health IT software and systems **25**
Bibliography and cited references **28**

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
Maureen Dailey, American Nurses Association
Richard De La Cruz, Silver Lake Group Inc
Sherman Eagles, SoftwareCPR
Neil Gardner, EHealth Saskatchewan
Richard Gibson, Association of Medical Directors of Information Systems
Peter Goldschmidt, World Development Group Inc
Karoll Gonzalez, Stryker Instruments Division
Susan Harkness Regli, University of Pennsylvania Health System
Zach Hettinger, MedStar Health Corporate Office
Rob Hyatt, Intermountain Healthcare
Michelle Jump, Nova Leah Ltd
Priti Lakhani, Cerner Corporation
Lana Lowry, National Institute of Standards & Technology
Anqi Lu, Pew Charitable Trust
Michael McCoy, McCoy, Lawrenceville, Georgia
Morgan Opie, Maryland Department of Health & Mental Hygiene
Anna Orlova, American Health Information Management Association
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
Gretchen Tegethoff, Knowledge Alliance
Matt Weinger, Vanderbilt University Medical Center
Michael Wiklund, UL LLC
Mike Willingham, 98point6 Inc
Marisa Wilson, Alliance for Nursing Informatics (ANI)
Ben Xavier, ICU Medical Inc
Karen Zimmer, Independent expert

Alternates:
Jeremy Jensen, Boston Scientific Corporation
S. Vivek, ICU Medical Inc
Walter Suarez, Kaiser Foundation Health Plan/Hospitals
Mala Ramaiah, National Institute of Standards & Technology
Beth George, Philips
Brian Pate, SoftwareCPR
Limor Hochberg, UL LLC
Andrew Gettinger, US Dept of Health & Human Services

Liaisons:
Diana Warner, American Health Information Management Association
Jeme Ertl, Hill-Rom
Diane Wurzburger, GE Healthcare
Beth Pumo, Kaiser Foundation Health Plan/Hospitals
Patty Krantz-Zuppan, Medtronic Inc Campus

Dave Osborn, Philips
Elizabeth Quill, Independent expert
Sandy Hedberg, SoftwareCPR
Frank Pokrop, Sotera Wireless Inc

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

This standard, HIT1000-1, *Safety and effectiveness of health IT software and systems—Part 1: Fundamental concepts, principles, and requirements*, is published as a provisional National Standard—a standard for trial use—and must be processed as a full American National Standard within 2 years of its publication date (see front cover).

This document has been processed in accordance with ANSI's requirements for a Provisional American National Standard. The Provisional Standards will undergo the standards development process set forth in AAMI's accredited procedures. This Provisional ANS or pertinent Provisional Amendment(s) shall be withdrawn on or before 5 October 2020.

Comments on this standard or suggestions for improving it are invited. Comments and suggested revisions should be sent to Technical Programs, AAMI, 4301 N. Fairfax Drive, Suite 301, Arlington, VA 22203-1633 or by email to standards@aami.org.

Introduction

Note: This introduction does not contain provisions of AAMI HIT1000-1 (PS), *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 usability 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.

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 this triad (e.g., ISO 9001:2015 or ISO 31000:2009), 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 lifecycle.[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 need for standards specific to health IT. The AAMI HIT1000 series is intended to address this need. The standards supplement existing quality management systems, risk management frameworks, and human factors engineering processes. They also facilitate shared responsibility among stakeholders by identifying specific roles and defining the responsibilities needed to ensure health IT safety and quality. The HIT1000 series will provide a common framework for cooperation and collaboration among the many organizations and individuals that develop, implement, and use health IT.

The AAMI HIT1000 series (*Safety and effectiveness of health IT software and systems*) is envisioned to initially comprise 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] 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 HIT1000-3, in development). 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 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 is an attribute 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, 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 lifecycle 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 lifecycle 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 lifecycle. At those stages, the HDO would also be serving as 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 lifecycle. 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.