American National Standard

ANSI/AAMI SW96:2023

Standard for medical device security—Security risk management for device manufacturers

AAMI
Advancing Safety in Health Technology

Standard for medical device security—Security risk management for device manufacturers

Approved 21 December 2022 by
AAMI

Approved 13 January 2023 by
American National Standards Institute, Inc.

Abstract: Provides requirements on methods to perform security risk management for a medical device in the context of the safety risk management process required by ISO 14971. This document is intended to be used in conjunction with AAMI TIR57 and AAMI TIR97.

Keywords: medical device, information security, security risk management

AAMI Standard

This Association for the Advancement of Medical Instrumentation (AAMI) standard implies a consensus of those substantially concerned with its scope and provisions. The existence of an 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 the standard. AAMI standards are subject to periodic review, and users are cautioned to obtain the latest editions.

CAUTION NOTICE: This AAMI standard may be revised or withdrawn at any time. AAMI procedures require that action be taken to reaffirm, revise, or withdraw this document no later than five years from the date of publication. Interested parties may obtain current information on all AAMI standards by calling or writing AAMI.

All AAMI standards, recommended practices, technical information reports, 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

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

Printed in the United States of America

ISBN 978-1-57020-862-1

Contents

Page

Annexes

Figures

Committee representation

Association for the Advancement of Medication Instrumentation

AAMI Medical Device Security Working Group

This AAMI American National Standard (ANS) was developed and approved by the AAMI Medical Device Security Working Group.

At the time this document was published, the **AAMI Medical Device Security Working Group** had the following members:

Cochairs: Brian Fitzgerald
Michael Seeberger

Members: Daniel Black, ResMed Inc.
Ryan Burke, AJW Technology Consultants Inc
Nick Chozos, Adelard LLP
Martin Crnkovich, Fresenius Medical Care
David Deaven, GE Healthcare
Cody DeGroot, Hennepin Healthcare System
Stephanie Domas, MedSec
Sherman Eagles, SoftwareCPR
Charles Farlow, Farlow Systems Consulting, LLC
Brian Fitzgerald, FDA/CDRH
Alex Forward, SunTech Medical Inc
Alan Fryer, Micro Systems Engineering Inc
Kevin Fu, Archimedes Center for Healthcare and Device Security
John Giantsidis, CyberActa Inc
Stephen Grimes, ABM Healthcare Services
David Guffrey, Mass General Brigham
Bob Haack, Karl Storz Endoscopy
Robert Haack, Johnson & Johnson
Christopher Howard, Medical Sensor Systems, Inc.
Michael Jaffe, Cardiorespiratory Consulting LLC
Michelle Jump, MedSec
Joshua Kim, Hill-Rom Holdings
Matthew Kirkwood, Smiths Medical
Adam Lacy, Stryker Instruments Division
Juuso Leinonen, ECRI Institute
Yimin Li, Abbott Laboratories
Dan Lyon, Synopsys Inc
Matthew McKenna, Draeger Medical Systems Inc.
Vidya Murthy, MedCrypt
Scott Nichols, Beckman Coulter Inc.
Susumu Nozawa, Siemens Healthineers
Chinemi Ochiai, Medtronic Inc
Brodie Pedersen, Borderless Compliance LLC
Andrea Ruth, ALR Consulting LLC
Michael Seeberger, Boston Scientific Corporation
Eirene Shipkowitz Smith, Baxter Healthcare Corporation
Jason Shutt, Olympus America Inc
Nick Sikorski, Deloitte Advisory
Chaitanya Srinivasamurthy, ICU Medical Inc
Sandra Stuart, Kaiser Foundation Health Plan/Hospitals
Eugene Vasserman, Kansas State University
David Vershum, Cantel Inc
Fubin Wu, GessNet
Daidi Zhong, Chongqing University
Charles Zinsmeyer, 3M Health Care

Alternates:
Alireza Ashani, Amgen Inc
Robert Banta, Eli Lilly & Company
Justin Bushko, AJW Technology Consultants Inc
John Dwyier, Onclave Network Inc
Phillip Englert, Deloitte Advisory
Dawn Flakne, Micro Systems Engineering Inc
Clark Fortney, Battelle Memorial Institute
Edwin Heierman, Abbott Laboratories
Curtice Huntington, Smiths Medical
Mitchell Kiklas, 3M Health Care
Rakesh Paruthikkat, STERIS
Sagar Patel, Battelle Memorial Institute
Chris Reed, Medtronic Inc Campus
Scott Robertson, Kaiser Foundation
Mark Rohlwing, ICU Medical Inc
Lisa Simone, FDA/CDRH
Robert Smigielski, B Braun of America Inc
Varun Verma, Philips
Loren Walkington, Cardinal Health
Grace Wiechman, Boston Scientific Corporation
Nicole Zuk, Siemens Healthineers

Liaisons:
Keith Anderson, Smiths Medical
Pat Baird, Philips
Tatiana Correia, 3M Health Care
Darren Dahlin, Cantel Inc
Anura Fernando, UL LLC
Zack Hornberger, Medical Imaging & Technology Alliance (MITA) a Division of NEMA
Kenneth Hoyme, Boston Scientific Corporation
Ujjwal Jain, Illumina Incorporated
Tara Larson, Abbott Laboratories
Jyh-Shyan Lin, DexCom Inc
Paul Matsumura, SunTech Medical Inc
Avital Merl, Becton Dickinson & Company
Komala Mullapudi, DexCom Inc
David Osborn, Philips
Robert Phillips, Siemens Healthineers
Umesh Shah, Abbott Laboratories
Donna Walsh, FDA/CDRH

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 document was developed by the AAMI Medical Device Security Working Group.

The challenge of managing *security risk*s for *medical devices* throughout their *life cycle* is becoming more complex. To develop *medical devices* and systems cost effectively, the use of a larger set of commercial third-party components during the development of a *medical device* is becoming more common, particularly for *medical devices* that are intended to be connected to networks. The result is that the overall *security risk* for a *medical device* evolves over time even if the *medical device* does not change. Knowledge of new *vulnerabilities* and *threats* can originate from multiple sources. *Manufacturers* need to be prepared to receive *vulnerability* information, actively seek information on new *threats*, assess *risk*, and take the appropriate action.

Accordingly, *security risk management* of *medical devices* is a total product *life cycle* activity.

The objective of this document is to specify requirements based on the guidance provided in the subordinate AAMI TIR57 [3] and AAMI TIR97 [4] on how *medical device manufacturers* should manage *security risk* throughout the *life cycle* of a *medical device* within the *risk management* framework defined by ISO 14971.

The following verbal forms are used within AAMI documents to distinguish requirements from other types of provisions in the document:

- "shall" and "shall not" are used to express requirements;
- "should" and "should not" are used to express recommendations;
- "may" and "may not" are used to express permission;
- "can" and "cannot" are used as statements of possibility or capability;
- "must" is used for external constraints or obligations defined outside the document; "must" is not an alternative for "shall."

Suggestions for improving this document are invited. Comments and suggested revisions should be sent to Standards, AAMI, 901 N. Glebe Road, Suite 300, Arlington, VA 22203 or standards@aami.org.

Introduction

ISO 14971 specifies a process for *risk management* of *medical devices,* including software as a *medical device* and in vitro diagnostic (IVD) *medical devices*. The process described intends to assist *manufacturers* of *medical devices* to identify the *hazards* associated with the *medical device*, to estimate and evaluate the associated *risks*, to control these *risks*, and to monitor the *effectiveness* of the controls (see Clause 1 of ISO 14971).

This document was developed to provide additional guidance and requirements specific to the unique handling of *medical device security risks*. AAMI TIR57 [3] provides guidance for addressing *security risk*, primarily during the design *life cycle* phase, within the *risk management* framework defined by ISO 14971. AAMI TIR97 [4] provides additional guidance on the management of postmarket *security risk* and is complimentary to AAMI TIR57 [3]. While TIR 97 and TIR 57 are technical information reports, this document is a standard that provides specific requirements for managing *security* related *risk* across the total product *life cycle* but within the *risk management* framework defined by ISO 14971.

Following the approach developed in AAMI TIR57 [3], the definition of *harm* is considered from the perspective of ISO 14971. Also considered is *harm* from healthcare information technology (IT) standards, such as the ANSI/AAMI/IEC 80001 family. Because a *risk management* process that narrowly focuses on the traditional "physical injury or damage" definition can limit the scope of *security risk management*, this document incorporates the broader considerations that *risk*s include effects outside the traditional scope of patient physical *harm,* and can include "reduction of *effectiveness,*" and "breach of *data and systems security*" as extended in the ANSI/AAMI/IEC 80001 family of standards [6]. The relationship illustrated in AAMI TIR57 [3], Figure 2, "A Venn diagram showing the relationship between *security* and *safety risks*" is equally applicable to concepts presented in this document. Annex B provides additional background about the similarities and differences between *security* and *safety risk management*.

ISO/TR 24971 [23] describes a "production and *post-production* activities" that consist of three processes:

- information collection (Subclause 10.2);
- information review (Subclause 10.3); and
- actions (Subclause 10.4).

This document complements each of these processes by addressing the unique challenges associated with specifying and maintaining the *security* of a *medical device*.

The following supporting annexes are provided:

- Annex A: Rationale;
- Annex B: Similarities and differences between *safety risk management* and *security risk management*;
- Annex C: *Security risk management* report;
- Annex D: *Threat* modeling.
- Annex E: Third-Party Service Organizations and *Security*.
- Annex F: *Security risk* scoring based on *likelihood of occurrence*

Standard for medical device security—Security risk management for device manufacturers

1 Scope

This document provides requirements and guidance when addressing design, production and *post-production security risk management* for medical devices within the *risk management* framework defined by ISO 14971.

This document is intended to assist *manufacturers* and other users of the standard with the following:

- identifying *threats*, *vulnerabilities*, and *assets* associated with *medical devices* and their components and supply chain vendors;
- estimating and evaluating associated *security risks*;
- determining appropriate *security risk controls* to reduce *security risks*;
- verifying and monitoring the *effectiveness* of the *security risk controls*;
- establishing an enterprise-wide process to manage *security post-production* interactions with users and other stakeholders that ensures *security* of *medical devices* and systems used to provide medical care;
- creating design features that enable production and *post-production* management of *security risk* and effective integration with healthcare delivery organization (HDO) network *security* policies and technologies, or other operational contexts;
- coordinating communications with HDOs for *security risks;*
- understanding and communicating the *security* expectations from *manufacturers* to those who deploy their *medical devices* in a user environment;
- implementing processes to manage and monitor fielded *medical devices* containing either (1) traditional software (including firmware), (2) programmable logic, and (3) hardware for *security vulnerabilities*;
- implementing *security risk management* processes to 1) assess *security risk* in order to decide when action is required and 2) coordinate with *safety risk management* processes;
- coordinating with HDOs on *security risk management* activities;
- developing, implementing, and operationalizing a *coordinated vulnerability disclosure* process;
- implementing processes to manage *medical device security* patching; and
- planning for *medical device* retirement.

This document is applicable to the entire *life cycle* of a *medical device* including design, production, and *post-production* phases. *End of Support (EOS)* and *End of Guaranteed Support (EOGS)* are milestones in the *post-production* phase of the *medical device* and may vary according to differing market and jurisdictional factors.

This document expands on the information provided in Clause 10 “Production and *post-production* activities” of ISO/TR 24971 [23] by highlighting the need for proactive monitoring to assess *threats* and detect *vulnerabilities*. It references the coordinated *safety*/*security risk assessment* approach that was presented in Clause 9 of AAMI TIR57 [3], “Production and *post-production* information.”

