Technical Information Report

AAMI TIR97: 2019

Principles for medical device security—Postmarket risk management for device manufacturers

AAMI
Advancing Safety in Health Technology

Principles for medical device security—Postmarket risk management for device manufacturers

Approved 27 September 2019 by
AAMI

Abstract: Provides guidance on methods to perform postmarket security risk management for a medical device in the context of the Safety Risk Management process required by ISO 14971. This TIR is intended to be used in conjunction with AAMI TIR57:2016.

Keywords: medical device, information security, risk management, postmarket

AAMI Technical Information Report

A technical information report (TIR) is a publication of the Association for the Advancement of Medical Instrumentation (AAMI) Standards Board that addresses a particular aspect of medical technology.

Although the material presented in a TIR may need further evaluation by experts, releasing the information is valuable because the industry and the professions have an immediate need for it.

A TIR differs markedly from a standard or recommended practice, and readers should understand the differences between these documents.

Standards and recommended practices are subject to a formal process of committee approval, public review, and resolution of all comments. This process of consensus is supervised by the AAMI Standards Board and, in the case of American National Standards, by the American National Standards Institute.

A TIR is not subject to the same formal approval process as a standard. However, a TIR is approved for distribution by a technical committee and the AAMI Standards Board.

Another difference is that, although both standards and TIRs are periodically reviewed, a standard must be acted on—reaffirmed, revised, or withdrawn—and the action formally approved usually every five years but at least every 10 years. A TIR must be acted on and the action formally approved usually every three years.

A TIR may be developed because it is more responsive to underlying safety or performance issues than a standard or recommended practice, or because achieving consensus is extremely difficult or unlikely. Unlike a standard, a TIR permits the inclusion of differing viewpoints on technical issues.

CAUTION NOTICE: This AAMI TIR may be revised or withdrawn at any time. Because it addresses a rapidly evolving field or technology, readers are cautioned to ensure that they have also considered information that may be more recent than this document.

All 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.

Comments on this technical information report are invited and should be sent to AAMI, Attn: Standards Department, 901 N. Glebe Road, Suite 300, Arlington, VA 22203.

Published by

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

Printed in the United States of America

ISBN 978-1-57020-725-9

Contents

Page

Committee representation

Association for the Advancement of Medical Instrumentation
AAMI Medical Device Security Working Group

This technical information report (TIR) 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:
Geoffrey Pascoe
Brian Fitzgerald, FDA/CDRH

Members:
AJ Aspinwall, Norton Healthcare
Daniel Black, ResMed Inc.
William Brodbeck, STERIS Corporation| Healthcare
Richard Brooks, Battelle Memorial Institute
Bill Brown, Spacelabs Healthcare
Ryan Burke, AJW Technology Consultants Inc
Nick Chozos, Adelard LLP
Martin Crnkovich, Fresenius Medical Care
David Deaven, GE Healthcare
Margaret DePuydt, 3M Healthcare
Stephanie Domas, MedSec
Sherman Eagles, SoftwareCPR
Plamena Entcheva-Dimitrov, Preferred Regulatory Consulting
Inc Charles Farlow, Medtronic Inc Campus
Philip Fasano, Onclave Network Inc
Brian Fitzgerald, FDA/CDRH
Phil Fisk, Baxter Healthcare Corporation
Jill French
Alan Fryer, Micro Systems Engineering Inc
Kerry Griffin, Stryker Instruments Division
Stephen Grimes, ABM Healthcare Services
David Guffrey, Partners Healthcare
Michael Jaffe, Cardiorespiratory Consulting LLC
Michelle Jump, Nova Leah Ltd
Joshua Kim, Hill-Rom Holdings
Matthew Kirkwood, Smiths Medical
Tara Larson, Eli Lilly and Company
Joseph Lashway, Oregon Biomedical Association
Juuso Leinonen, ECRI Institute
Yimin Li, Abbott Laboratories
Joern Lubadel, B Braun of America Inc
Dan Lyon, Synopsys Inc
Matthew McMahon, Siemens Healthineers
Michael McNeil, Philips
Vidya Murthy, MedCrypt
Susumu Nozawa, Siemens Healthineers
Sagar Patel, Battelle Memorial Institute
Geoffrey Pascoe
Brodie Pedersen, Borderless Compliance LLC
Mike Powers, Christiana Care Health Srvcs
Chad Quistad, Regulatory and Quality Solutions LLC
Andrea Ruth, ALR Consulting LLC
Michael Seeberger, Boston Scientific Corporation
Nick Sikorski, Deloitte Advisory
Sandra Stuart, Kaiser Foundation Health Plan/Hospitals

David Vershum, Cantel Inc
Fubin Wu, GessNet
Susan Yang, Amgen Inc
Daidi Zhong, Chongqing University

Alternates:

Robert L. Banta, Eli Lilly and Company
Justin Bushko, AJW Technology Consultants Inc
John Dwyier, Onclave Network Inc
Phillip Englert, Deloitte Advisory
Dawn Flakne, Micro Systems Engineering Inc
Karoll Gonzalez, Stryker Instruments Division
Edwin Heierman, Abbott Laboratories
Curtice Huntington, Smiths Medical
Alexander Kent, Medtronic Inc Campus
Gregory Land, STERIS Corporation| Healthcare
Dale Nordenberg, MDISS—Medical Device Innovation, Safety and Security Consortium Jyothsna Nunna, Regulatory and Quality Solutions LLC
Beth Pumo, Kaiser Foundation Health Plan/Hospitals
Mark Rohlwing, ICU Medical Inc
Lisa Simone, FDA/CDRH
Robert Smigielski, B Braun of America Inc
Ryan Wick, Deloitte Advisory
Grace Wiechman, Boston Scientific Corporation
Ashley Woyak, Baxter Healthcare Corporation
Jaime Zappa, Cantel Inc
Nicole Zuk, Siemens Healthineers
Varun Verma, Philips

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 technical information report (TIR) was developed by the AAMI Device Security Working Group.

The challenge of managing security risks for deployed devices is becoming more complex. To develop 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 devices that are intended to be connected to networks. The result is that the security risk for a device evolves over time even if the 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.

The objective of this TIR is to provide guidance on how medical device manufacturers should manage security risk in the production and post-production phases of the life-cycle of a medical device within the risk management framework defined by ANSI/AAMI/ISO 14971:2007. TIR97 is intended to be used in conjunction with AAMI TIR57:2016.

Suggestions for improving this recommended practice are invited. Comments and suggested revisions should be sent to Technical Programs, AAMI, 901 N. Glebe Road, Suite 300, Arlington, VA 22203.

NOTE This foreword does not contain provisions of AAMI TIR97, *Principles for medical device security—Postmarket risk management for device manufacturers* (AAMI TIR97:201x), but it does provide important information about the development and intended use of the document.

Introduction

ANSI/AAMI/ISO 14971:2007(R)2010 is an integral part of the safety risk management processes required by many regulatory authorities. ANSI/AAMI/ISO 14971 specifies a process for a manufacturer to identify the hazards associated with medical devices, including in vitro diagnostic (IVD) medical devices, to estimate and evaluate the associated risks, to control these risks, and to monitor the effectiveness of the controls (see Clause 1 of ANSI/AAMI/ISO 14971:2007).

AAMI TIR57:2016—*Principles for medical device security—Risk management* provides guidance for addressing security within the risk management framework defined by ANSI/AAMI/ISO 14971. This report augments AAMI TIR57 by providing detailed guidance for the management of security risks in the production and post-production phases of the life-cycle of a medical device.

Following the approach developed in AAMI TIR57:2016, the definition of harm is considered from the perspective of ANSI/AAMI/ISO 14971, as well as from healthcare information technology (IT) standards, such as the ANSI/AAMI/IEC 80001 family. Because a security risk management process that narrowly focuses on the traditional "physical injury or damage" definition can limit the scope of security risk mitigation, this document incorporates the broader considerations that risks 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. The relationship illustrated in AAMI TIR57:2016, Figure 2, "A Venn diagram showing the relationship between security and safety risks" is equally applicable to concepts presented in this report.

ANSI/AAMI/ISO TIR24971:2013/(R)2016 *Medical devices—Guidance on the application of ISO 14971* describes a "production and post-production feedback loop" that consists of three processes:

- observation and transmission (Subclause 4.2);
- assessment (Subclause 4.3); and
- action (Subclause 4.4).

This report expands upon each of these processes to address the unique challenges associated with maintaining the security of a medical device.

Supporting annexes contain the following:

- Annex A: Sample medical device security policy statements—Provides a non-exhaustive list of sample statements that can be incorporated in a manufacturer's medical device security policy;
- Annex B: Security risk management for healthcare networks—An overview of risk control measures that can be implemented by a healthcare delivery organization and in the home networking environment;
- Annex C: Establishing a coordinated vulnerability disclosure process—Reviews manufacturer-specific considerations for establishing a coordinated vulnerability disclosure process based on published vulnerability disclosure and vulnerability handling consensus standards; and
- Annex D: Mapping of defined terms included in Guidance for Industry and Food and Drug Administration Staff, Postmarket Management of Cybersecurity in Medical Devices—A comparison of terms defined in FDA guidance with those defined in ANSI/AAMI/ISO 14971:2007 and this report.

Principles for medical device security—Postmarket risk management for device manufacturers

1 Scope

This TIR provides guidance for addressing postmarket security risk management within the risk management framework defined by ANSI/AAMI/ISO 14971. While it is based on the ANSI/AAMI/ISO 14971 framework for medical device risk management, most concepts are applicable to any healthcare product that requires postmarket management of security.

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

- establishing an enterprise-wide process to manage security postmarket interactions with users and other stakeholders;
- creating design features that enable postmarket management of security risk and effective integration with healthcare delivery organization (HDO) network security policies and technologies, or other operational contexts;
- understanding and communicating the security expectations from manufacturers to those who deploy medical devices in a user environment;
- implementing processes to monitor fielded devices for newly discovered security vulnerabilities both from the devices themselves and from other sources;
- implementing processes to assess both safety and security risk to decide when action is required;
- developing a coordinated vulnerability disclosure process;
- implementing processes to manage device security patching; and
- planning for device retirement.

The guidance provided by this document is applicable to the production and post-production phases of the life-cycle of a medical device (hereinafter referred to as the “postmarket” phase).

This TIR expands the information provided in Clause 4 “Production and post-production feedback loop” of ANSI/AAMI/ISO TIR24971:2013 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 TIR57:2016, Production and post-production information.

2 Terms and definitions

For the purposes of this document, the terms and definitions given in AAMI TIR57:2016 and the following apply.

2.1
accompanying document
document accompanying a medical device and containing information for those accountable for the installation, use, and maintenance of the medical device, the operator, or the user, particularly regarding safety

NOTE Adapted from IEC 60601-1:2005, definition 3.4.

[SOURCE: ISO 14971:2007, 2.1]