

Technical Information Report

AAMI TIR97: 2019

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

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that, although both standards and TIRs are periodically reviewed, a standard must be acted on—reaffirmed, revised, or withdrawn—and the action formally approved usually every five years but at least every 10 years.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CAUTION NOTICE: This AAMI TIR may be revised or withdrawn at any time.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

© 2019 by the Association for the Advancement of Medical Instrumentation

All Rights Reserved

This publication is subject to copyright claims of AAMI. No part of this publication may be reproduced or distributed in any form, including an electronic retrieval system, without the prior written permission of AAMI. All requests pertaining to this document should be submitted to AAMI. It is illegal under federal law (17 U.S.C. § 101, et seq.) to make copies of all or any part of this document (whether internally or externally) without the prior written permission of the Association for the Advancement of Medical Instrumentation. Violators risk legal action, including civil and criminal penalties, and damages of \$100,000 per offense. For permission regarding the use of all or any part of this document, complete the reprint request form at www.aami.org or contact AAMI, 901 N. Glebe Road, Suite 300, Arlington, VA 22203. Phone: +1-703-525-4890; Fax: +1-703-276-0793.

Printed in the United States of America

ISBN 978-1-57020-725-9

Contents	Page
Committee representation	iv
Foreword	vi
Introduction	vii
1 Scope.....	1
2 Terms and definitions.....	1
3 Postmarket considerations for security policies and security program administration.....	4
4 Design features for postmarket security risk management	5
5 Installation and configuration	5
6 Postmarket management of fielded devices	6
7 Retirement/obsolescence	19
Annex A (informative) Sample medical device security policy statements.....	22
Annex B (informative) Security risk management for healthcare networks	25
Annex C (informative) Establishing a coordinated vulnerability disclosure process	32
Annex D (informative) Mapping of defined terms included in Guidance for Industry and Food and Drug Administration Staff, Postmarket Management of Cybersecurity in Medical Devices	35
Annex E (informative) Security incident handling and response	40
Bibliography	46

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 Svcs
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]

2.2

compensating risk control measure

compensating control

specific type of risk control measure deployed in lieu of, or in the absence of, risk control measures implemented as part of the device's design

Note 1 to entry: A compensating risk control measure could be permanent or temporary (e.g., until the manufacturer can provide an update that incorporates additional risk control measures).

[SOURCE: Guidance for Industry and Food and Drug Administration Staff, Postmarket Management of Cybersecurity in Medical Devices (2016), modified—The first sentence of definition IV.A has been incorporated with changes to clarify that this type of risk control measure is not part of the device's design. Note 1 to entry has been added to delineate different types of measures.]

2.3

coordinated vulnerability disclosure

CVD

process through which researchers and other interested parties work cooperatively with a manufacturer in finding solutions that reduce the risks associated with disclosure of vulnerabilities

Note 1 to entry: This process encompasses actions such as reporting, coordinating, and publishing information about a vulnerability and its resolution.

[SOURCE: ISO 29147:2014, modified—Adapted from text contained within the introduction clause.]

2.4

cybersecurity signal

information that indicates the potential for, or confirmation of, a vulnerability, exploit, threat, or threat event that affects, or could affect, a medical device.

[SOURCE: Guidance for Industry and Food and Drug Administration Staff, Postmarket Management of Cybersecurity in Medical Devices (2016), modified—The first sentence of definition IV.D has been incorporated with changes to add threat and threat event.]

2.5

end of guaranteed support

EOGS

point at after which the manufacturer no longer guarantees full support.

Note 1 to entry: During this life-cycle stage, there can be some level of support available by the manufacturer, but without a guarantee that the medical device can be maintained to its original specification and performance.

2.6

end of support

EOS

point after which the manufacturer terminates all service support activities

Note 1 to entry: Service support does not extend beyond this point.

2.7

exploit

instance where a vulnerability or vulnerabilities have been exercised (accidentally or intentionally) by a threat

SOURCE: Guidance for Industry and Food and Drug Administration Staff, Postmarket Management of Cybersecurity in Medical Devices (2016), modified—Definition IV.E has been changed to remove language pertaining to potential impacts.]

Note 1 to entry: "Exploit" can also be a technique that exercises a security vulnerability.

2.8

guaranteed support

life-cycle stage of a product starting with customer availability in the post-production phase and ending when the product reaches the point at which the manufacturer no longer guarantees full support

Note 1 to entry: Limited support can be available once a medical device reaches the end of guaranteed support depending upon the manufacturer, medical device, and other factors.

2.9

information sharing and analysis center

ISAC

operational entities formed by critical infrastructure owners and operators to gather, analyze, appropriately sanitize, and disseminate intelligence and information related to critical infrastructure

Note 1 to entry: ISACs provide 24/7 threat warning and incident reporting capabilities and have the ability to reach and share information within their sectors, between sectors, and among government and private sector stakeholders.

Note 2 to entry: ISACs are the original ISAOs for the critical infrastructure sectors.

Note 3 to entry: Although ISACs are recognized as operational entities in the United States, similar organizations exist in other countries.

[SOURCE: U.S. Department of Homeland Security, National Infrastructure Protection Plan 2013, modified—The second sentence has been moved to a note (Note 1 to entry). Note 2 to entry and Note 3 to entry have been added to clarify applicability. The source for Note 2 to entry is <https://nhisac.org/nhisac-faq/>.]

2.10

information sharing and analysis organization

ISAO

any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of gathering, analyzing, communicating, disclosing, or voluntarily disseminating information in order to better understand security problems and interdependencies related to critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability thereof

Note 1 to entry: An ISAO communicates or discloses critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or an incapacitation problem related to critical infrastructure or protected systems.

Note 2 to entry: An ISAO voluntarily disseminates critical infrastructure information to its members, local and Federal Governments, or any other entities that may be of assistance. Similar organizations exist in other countries.

[SOURCE: 6 U.S.C § 131 (5), modified—The definition has been developed from subparagraph (a) modified to include progressive verbs of subparagraphs (b) and (c). Note 1 to entry and Note 2 to entry have been added to summarize subparagraphs (b) and (c), respectively, and to clarify applicability.]

2.11

intended use

intended purpose

use for which a product, process or service is intended according to the specifications, instructions, and information provided by the manufacturer

[SOURCE: ANSI/AAMI/ISO 14971:2007, definition 2.5]

2.12

life-cycle

all phases in the life of a medical device, from the initial conception to final decommissioning and disposal

[SOURCE: ANSI/AAMI/ISO 14971:2007, definition 2.7]

2.13

post-production

part of the life-cycle of the product after the design has been completed and the medical device has been manufactured

EXAMPLES transportation, storage, installation, product use, maintenance, repair, product changes, decommissioning and disposal.

Note 1 to entry: The post-production phase includes devices manufactured and placed in inventory as well as those devices that have been shipped to customers and are subject to postmarket surveillance.

[SOURCE: ANSI/AAMI/ISO 14971:2007, definition 2.11, modified—Note 1 to entry has been added.]

2.14

security capability

The broad category of technical, administrative or organizational controls to manage risks of confidentiality, integrity, and availability and accountability of data and systems.

[SOURCE: ISO/IEC 80001-2-2: XXXXXXXXX]

2.15

security incident

a violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices

[SOURCE: NIST SP 800-61 Rev. 2 (2012), modified—The term “computer” has been removed from the definition included in section 2.1.]

3 Postmarket considerations for security policies and security program administration

3.1 Medical device security policy

AAMI TIR57:2016 provides guidance on developing a medical device security policy in Subclause 3.2, Management responsibilities. The medical device security policy should define management’s intent to secure the organization’s medical devices throughout their lifecycle. The policy should address postmarket regulatory requirements and be supported by standards, procedures, work instructions, and other artifacts that address security risk management, threat event handling, incident handling, coordinated vulnerability disclosure, and security education and training. In addition, the policy should facilitate consistent and effective external communications, as well as allow for monitoring and improvement of the processes required by the policy.

Postmarket information in the policy should include, but not be limited to, threat intelligence, patch and vulnerability management, threat event and incident handling, security risk assessment, and third-party risk management. The policy should also include requirements for security maintenance across the entire device life-cycle.

Annex A provides a non-exhaustive list of sample statements that can be incorporated in a manufacturer’s medical device security policy.

3.2 Coordinated vulnerability disclosure

Manufacturers should develop a coordinated vulnerability disclosure process to provide security researchers and others with a means to communicate device vulnerabilities to appropriate parties, including regulatory authorities.

Subclause 6.1.2 and Annex C provide additional information about establishing a coordinated vulnerability disclosure process.

NOTE The customer communication channel for handling complaints can typically be used for handling reports of potential vulnerabilities with minor modifications and appropriate training. However, this is separate from the coordinated vulnerability disclosure process which requires agreements to be in place prior to discussion of vulnerabilities.

3.3 Information sharing

Information about medical device vulnerabilities and potential threats to these devices should be communicated in a consistent manner to existing customers. Depending on the nature of the vulnerability or threat, it may also be important, such as when the vulnerability or threat could apply to the broader industry, to share the information with an information sharing and analysis organization (ISAO).

To prevent threat actors from exploiting a vulnerability in a device and potentially causing harm, a process should be established to communicate details on vulnerabilities, compensating controls, and risk controls to customers. How quickly this communication will occur should be established and be dependent on risk level of the vulnerability/threat. In the case of a moderate to high-risk vulnerability, communication to the customer should be done expediently even if vendor-recommended compensating controls or remediation steps are not yet available (see Subclause 6.2.2). This communication may include posting known vulnerabilities to a publicly accessible or password protected space (i.e., company website) together with the corresponding patches, when applicable. Information provided may also be staged as it becomes available. Information shared should also include details about the risk ranking of the vulnerability (e.g., its Common Vulnerability Scoring System(CVSS) scoring) and whether it has been exploited. For

higher-risk vulnerabilities, the first stage will typically suggest compensating controls (e.g., removing the medical device from the network) that can be implemented by the end user while the manufacturer develops a more comprehensive risk control measure (e.g., patch). For a high-profile vulnerability which affects the overall medical and IT industries (e.g., WannaCry), even if the manufacturer confirms that the vulnerability is not exploitable on their product(s), the manufacturer should promptly communicate this information in order to assist HDOs in concentrating their efforts on other medical devices potentially affected. Reporting vulnerabilities to an ISAO allows critical cyber information to be shared with other stakeholders, which can prevent similar vulnerabilities in other medical devices from being exploited or additional cyber-attacks from occurring. This relationship is mutual, and in return for sharing information, manufacturers should be given information and intelligence on vulnerabilities and threats across multiple sectors.

3.4 Communication of security capabilities

Potential customers often send inquiries to manufacturers requesting the security capabilities of products under consideration. The manufacturer should establish and maintain a process for providing potential, and existing, customers with current and accurate security capability documentation. The format and content of this documentation should be consistent. An accurate software bill of materials (SBOM) is a key component for creating a product security risk assessment, performing technical security testing, monitoring of threats and vulnerabilities, and responding effectively to threat events. An SBOM also supports HDOs in establishing an inventory of medical devices, including software.

NOTE A Security Bill of Materials (CBOM) would include hardware sub-components in addition to the SBOM. In this document we will continue to use the term SBOM because it is well understood.

A common way to communicate the security capabilities of medical devices is the Manufacturer Disclosure Statement for Medical Device Security (MDS2) form [6]. The value of the MDS2 form depends on the level of detail provided in the “notes” sections for each security capability. In many cases, customers request detailed information about security capabilities of medical devices in their own format. The manufacturer should be prepared to respond to these requests in a timely manner. Some requests could necessitate the development of contractual provisions to protect the intellectual property of the manufacturer.

To facilitate timely responses to detailed customer inquiries, manufacturers should describe the security capabilities of a device in a standardized format, in a template with consistent language between product teams, during the product generation/creation process. This information supports the preparation of MDS2 forms for the product and can form the basis of standard responses to customer inquiries. MDS2 forms should be made available to customers upon request, and updated forms should be released whenever security capabilities are modified due to new product or version releases.

4 Design features for postmarket security risk management

As defined in ISO 14971, risk management includes “activities related to collection and review of relevant production and post-production information.” The device should include features that enable the collection of information relevant to management of post-production security risk or otherwise enable oversight and protection. While HDO networks share characteristics of IT networks, it is incumbent on the manufacturer to understand, where possible, the operational context.

Annex B provides an overview of risk control measures that can be implemented by a manufacturer to support HDOs and home healthcare users. This annex is intended to complement standards such as IEC/TR 80001-2-2 *Application of risk management for IT-networks incorporating medical devices—Part 2-2: Guidance for the communication of medical device security needs, risks and controls* and IEC/TR 80001-2-8 *Application of risk management for IT-networks incorporating medical devices—Part 2-8: Application guidance—Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2*.

NIST Special Publication 800-160 *Volume 1 Systems Security Engineering* provides information on how to incorporate security-specific design features into the device during its development life-cycle. AAMI TIR57:2016 provides manufacturer-focused guidance in Annex C, Generating cybersecurity requirements.

5 Installation and configuration

AAMI TIR57:2016, Subclause 4.2, states that the manufacturer should document characteristics of the system that rely on user configuration to ensure the security of the device. Annex D of AAMI TIR57:2016 includes checklist items that address the secure installation and configuration of medical devices.

5.1 Device security configuration

Device security configurations can apply to a variety of device components, such as access control mechanisms (e.g., file permissions), cryptography modules, network devices (e.g., firewalls), malicious code protection (e.g., anti-virus or application whitelisting), and third-party software (e.g., operating system). A medical device should be designed with a baseline configuration which should be used to periodically check against the device's current configuration to determine if the configuration has been altered. The device's design should include features to allow a configuration difference to be determined. Policies, standards, and procedures should be developed to establish minimum hardening requirements and processes for the development, management, and ongoing monitoring of device component configurations. Device component configurations need to be managed and maintained per contract and service level agreements (e.g., the secure use and storage of a configuration).

Improper configuration of devices can introduce vulnerabilities that degrade confidentiality, integrity, or availability. Each device component configuration should be considered for hardening, including assessing whether hardening could affect critical functionality and/or performance of the component. If the component is hardened, industry practices should be leveraged whenever possible, such as security technical implementation guides (STIGs). Tools such as STIGs provide a robust mechanism for hardening third-party software. In addition, the device manufacturer should provide a hardened configuration for each device component (by default) and allow the customer to add or increase security settings of each configuration. Removing or decreasing security settings from the default, secure configuration should be discouraged. Customers should be cautioned against making changes to medical devices that result in higher security risk. Use both customer device documentation and/or warnings in the medical device. For example, a medical device could provide a warning if the changes to the configuration would result in higher security risk.

5.2 Security utility updating

Updates to security utilities such as network devices (e.g., firewalls) or malicious code protection mechanisms (e.g., anti-virus) need to be controlled. An improperly configured or malformed update can introduce vulnerabilities (e.g., accidentally opening firewall ports) or render a security utility unavailable. Updates should be tested in a staging environment, which mirrors a production environment, to determine if the update has any unintended consequences or impact to clinical functionality and capability of the device. After the update is tested, the manufacturer should distribute the update to all fielded devices that use the security utility. Updates should be deployed in alignment with service level agreements between the manufacturer and the HDO. If an update is not able to be deployed for any reason, an explicit business reason should be provided, and compensating security controls should be identified, documented, and communicated to the customer.

5.3 Other considerations for security maintenance in the clinical environment

Security maintenance provided in the clinical environment by the manufacturer should be logged and monitored using automated tools (e.g., security information and event monitoring (SIEM)). These automated tools should include functionality to allow for output to the end user, including a detailed log of changes that have been made to the device's security configuration. Security settings should not be changed without the explicit and documented authorization of the operator of the medical device. Security maintenance activities should be authenticated and be restricted from accessing unauthorized device functionality or data.

6 Postmarket management of fielded devices

When a medical device is in use, there are several sources of information through which a manufacturer can learn of vulnerabilities in, and threats to, fielded devices. It is important to understand that vulnerabilities exist in practically any software-controlled device. They can be present in the third-party code that is used in the device (e.g., operating system, networking libraries, frameworks) or in the code developed by the manufacturer. Discovery can come from both outside the manufacturer (e.g., researchers, suppliers, national databases) or from internally driven activities (e.g., failure analysis, engineering work, contracted device analysis, various testing activities).

After a vulnerability or threat is identified, it should be assessed for the risk to which it can expose the device, either in terms of safety and to the security of the device or to other systems on the network to which the device is connected.

Figure 1 extends Figure 4 from AAMI TIR57:2016 to add the postmarket decision-making that can trigger a reassessment of either safety or security risk (or both) and the decision whether a vulnerability requires correction, new threats are significant, and additional safety or security controls are required.

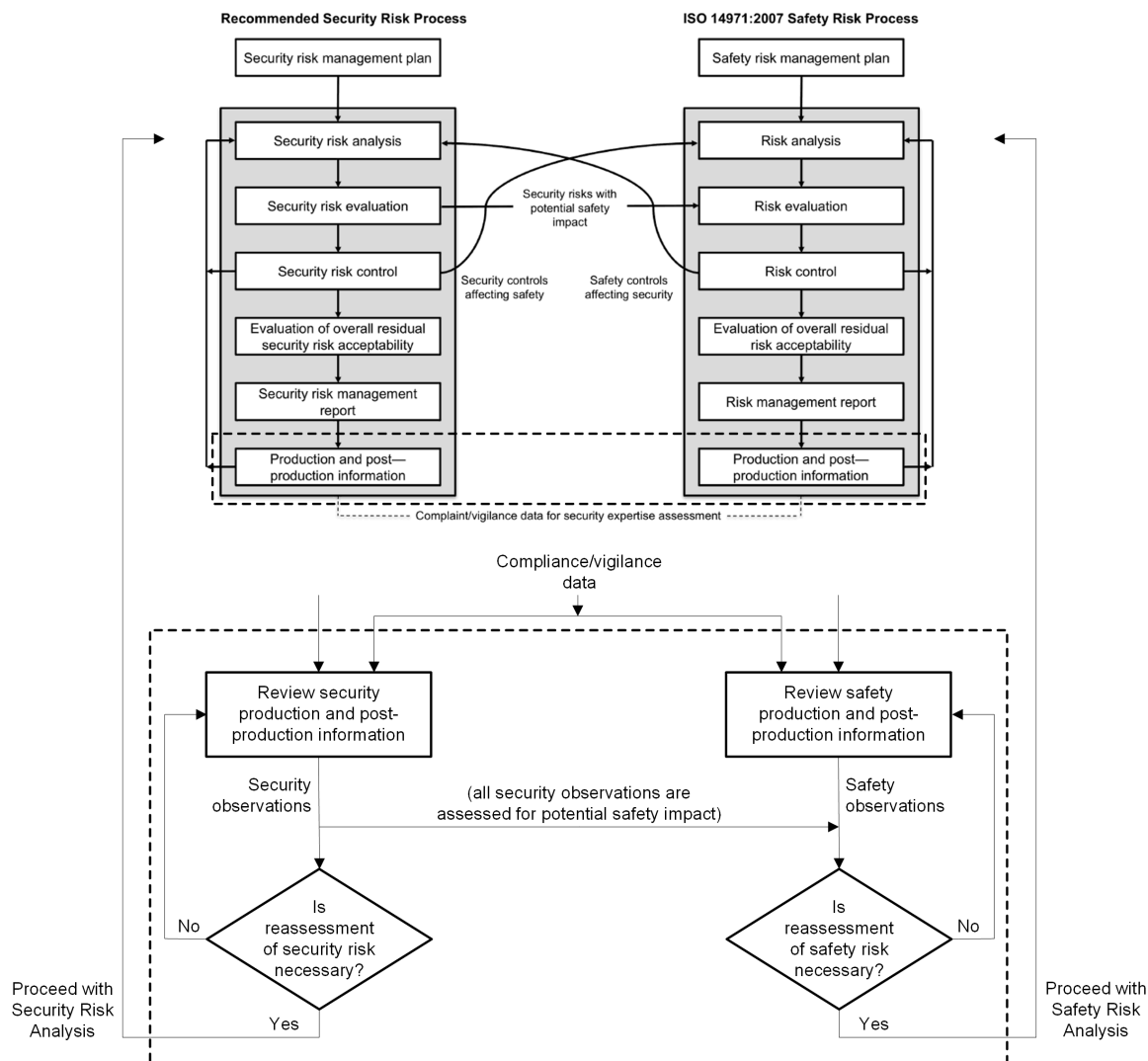


Figure 1—Postmarket decision-making flow diagram

This subclause covers the processes and decision steps a manufacturer should consider in creating their postmarket security response procedures. It is organized along the steps identified in Clause 4 of ANSI/AAMI/ISO TIR24971:2013:

- observation and transmission;
- assessment; and
- action.

Cybersecurity signals, as defined in Subclause 2.3, are a subset of “security production and post-production information” as illustrated in Figure 1. Cybersecurity signals can impact security risk assessments for multiple products. For each product-specific security risk assessment, a single cybersecurity signal can impact assessments for multiple threat events.

Before categorizing a signal as a security incident, triaging should occur to validate that there has been an attempt to access and/or adversely affect device data, systems, services, or networks in the context of data availability,