**AAMI CDV TIR97**

**Committee Draft for Comment**

AAMI Technical Information Report

**NOTE** - This document is still under study and subject to change.
It should not be used for reference purposes.

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

**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

**Association for the Advancement of Medical Instrumentation**
4301 N Fairfax Drive, Suite 301, Arlington VA 22203-1633
Phone 703/525-4890 Fax 703/276-0793 Internet www.aami.org

# Contents

# Foreword

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

The challenge of managing cybersecurity 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 to 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, 4301 N. Fairfax Drive, Suite 301, Arlington, VA 22203-1633.

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

Medical device manufacturers are familiar with the requirements of ANSI/AAMI/ISO 14971:2007/(R)2010 *Medical devices — Application of risk management to medical devices*. This standard 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 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, 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.
- 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.

# 1 Scope

This TIR provides guidance for addressing postmarket security 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 in the following:

- establishing a corporate level 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 their 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**
**compensating risk control measure**
**compensating control**
specific type of risk control measure recommended by the device manufacturer in lieu of, or in the absence of, risk control measures implemented by the device manufacturer

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 recommended by the device manufacturer. Note 1 to entry has been added to delineate different types of measures.]

**2.2**
**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 a vulnerability

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.]

**2.3**
**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.]

**2.4**
**end of life**
**EOL**
life-cycle stage of a product starting when the manufacturer no longer sells the product or guarantees full support

Note 1 to entry: There can be some level of support available by the manufacturer, but without guarantee that the medical device can be maintained to its original specification and performance.

**2.5**
**end of support**
**EOS**
life-cycle stage of a product starting when the manufacturer terminates all service support activities

Note 1 to entry: Service support contracts do not extend beyond this point. No service activities, paid repair, parts delivery or help desk support should be provided after a product has reached end of support.

**2.6**
**exploit**
instance where a vulnerability or vulnerabilities have been exercised (accidently 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.]

**2.7**
**guaranteed support**
life-cycle stage of a product starting with customer availability in the post-production phase and ending when the product reaches end of life

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

**2.8**
**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/.]

**2.9**
**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.]

**2.10**
**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]

**2.11**
**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]

**2.12**
**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.]

**2.13**
**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 the manufacturer’s high-level goals and objectives. The policy should conform to postmarket regulatory requirements and be supported by standards, procedures, work instructions, and other artifacts as needed that address security risk management, threat event, incident handling, 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. The manufacturer should utilize customer communication channels to enable customers and users to report potential vulnerabilities. At the discretion of the manufacturer, vulnerabilities should be reported to an information sharing and analysis organization, which could help stakeholders understand and mitigate potential widespread security risk.

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

To prevent threat actors from exploiting a device's vulnerability and potentially harming patients, vulnerabilities and patches should be communicated to the customer as early is practical (see Subclause 3.2). This may include posting known vulnerabilities to a publicly accessible or password protected space (i.e., company website) and the corresponding patches, when applicable, that resolve a security issue. Information provided may also be staged as it becomes available. The first stage typically suggests compensating controls that can be implemented by the end user while the manufacturer develops a more comprehensive risk control measure. If the notification addresses a global threat that is not exploitable on the product, this information can be shared immediately. Information should also include details about the risk ranking of a vulnerability (e.g. its CVSS scoring) and whether it has been exploited in the wild.

Reporting vulnerabilities to an ISAO allows critical cyber information to be shared with other stakeholders, which can prevent similar vulnerabilities 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 attributes

Potential customers often send inquiries to manufacturers requesting the security attributes of products under consideration. The manufacturer should establish and maintain a process for providing potential customers with current and accurate security attribute documentation. The format and content of this documentation should be consistent. A software bill of materials (SBOM) can assist in the completeness of a product security risk assessment, technical security testing, detailed monitoring of threats and vulnerabilities of the devices, and the timely and effective response to threat events. An SBOM also supports HDOs in establishing an inventory of medical devices, including software and hardware sub-components.

A common way to communicate the security attributes of medical devices is the Manufacturer Disclosure Statement for Medical Device Security (MDS2) form [6]. The value of the MDS2 form depends on the detail provided in the "notes" sections for each security capability. In many cases, customers request detailed information about security attributes of medical devices in their own format. The manufacturer should be ready to respond to these requests in a timely manner.

To facilitate timely response to detailed customer inquiries, manufacturers should describe the security properties of a device in a standard, internal, format 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 properties 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.” In this clause we discuss the device features that would 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 the deployment environment and the monitoring services specific to the HDO network.

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 SP 800-64 *Security Considerations in the System Development Life Cycle* provides information on how to incorporate security-specific design features into the device secure development life-cycle (SDLC). 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., Active Directory), 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 baseline configuration should be established and periodically checked against the device’s current configuration to determine if the configuration has been altered. 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 the 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 in both device documentation and, when appropriate, on the device itself when changes result in higher security risk, where the level of risk is determined by the security risk assessment.

## 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 provider. 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 recommended.

## 5.3 Other considerations for end user security maintenance

End user security maintenance provided 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. Maintenance personnel should not have the ability to remove or alter default security settings (unless increasing security settings). In addition, during security maintenance activities, maintenance personnel should be

restricted from accessing any other device functionality or data. Lastly, remote access for security maintenance activities should be explicitly approved/granted by the customer before a remote access session is fully established.

## 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 party code that is used in the device (operating system, networking libraries, frameworks, etc.) or in the code developed by the manufacturer. Discovery can come from outside the manufacturer (researchers, suppliers, national databases) or from internal or contracted device analysis and/or testing.

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, whether new threats are significant, and whether additional safety or security controls are required.

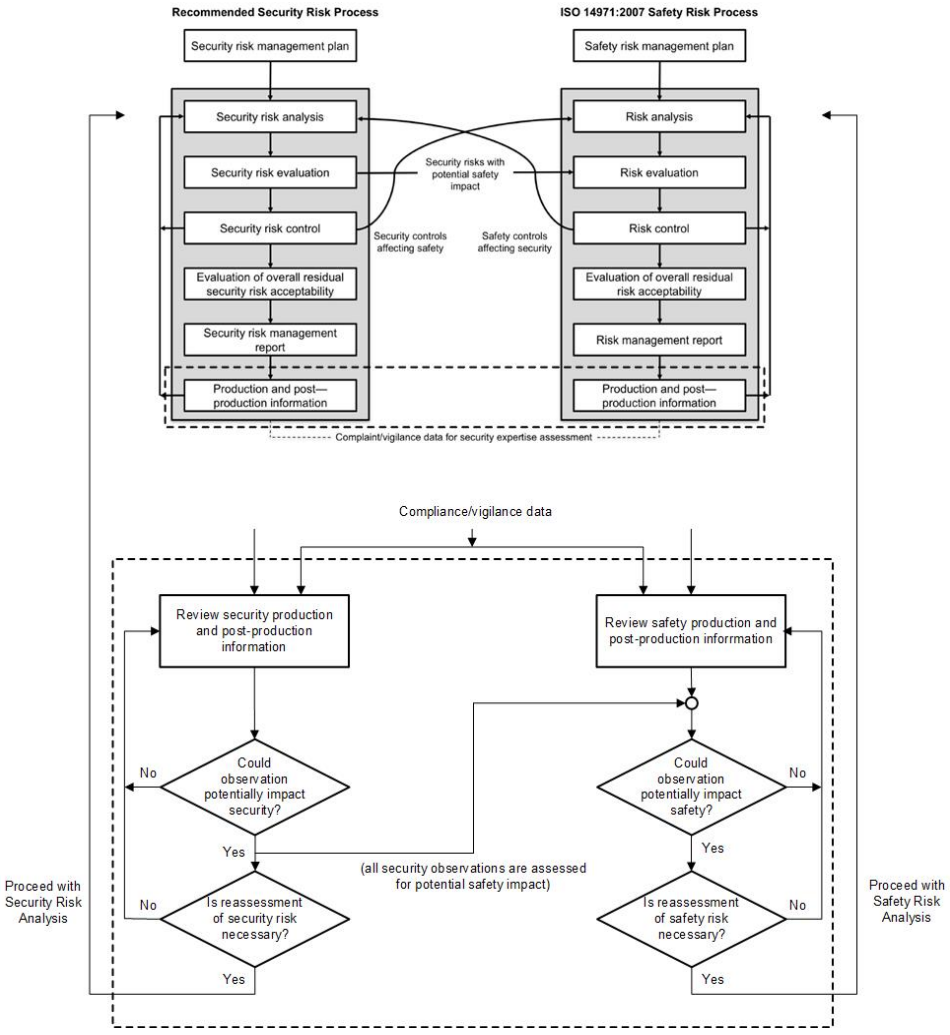


**Figure 1 — Postmarket decision-making flow diagram**

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;

425 — assessment; and

426 — action.

427 **6.1 Observation and transmission**

428 **6.1.1 Security monitoring**

429 Once a device is being marketed, the manufacturer is responsible for monitoring its on-going security status.
430 Information on potential sources of insecurity can come from several sources.

431 **6.1.1.1 Supplier monitoring**

432 An essential part of monitoring the security status of a device is the monitoring of software of unknown provenance
433 (SOUP), commercial off-the-shelf (COTS), and hardware vendors for reported defects, patches, and vulnerabilities.
434 The manufacturer should be aware of what SOUP and COTS is included in its products. The manufacturer should
435 develop a process for monitoring its suppliers for the availability of software updates, and for disclosure of
436 vulnerabilities and defects:

437 — examining release notes for new versions of the product to determine which defects have been corrected in
438 the earlier version;

439 — registering with the supplier (website) to get updates on specific products and versions, when available;

440 — reviewing trade publications and product-related bulletin boards for information.

441 Self-support can be necessary when the licensing for software explicitly excludes support, and the user becomes
442 responsible for resolving issues that are uncovered and maintenance of the software. On receiving notice of end of
443 support for any SOUP or COTS component, the manufacturer should review the usage of the software and develop a
444 plan to either replace the software or take over its maintenance.

445 **6.1.1.2 Vulnerability monitoring**

446 Vulnerabilities in third-party SOUP and COTS components and in the device manufacturer's software can be reported
447 by parties other than the supplier. The manufacturer should, at a minimum, monitor these sources:

448 — researchers that investigate and report vulnerabilities in health software and medical devices;

449 NOTE A coordinated vulnerability disclosure policy (see Subclause 3.2) is essential in managing interactions with
450 researchers.

451 — vulnerability databases such as ICS-CERT, US-CERT (general), and OWASP (web application);

452 — other vulnerability databases that are not focused on health software such as US-CERT and OWASP;

453 — incident response reporting from customers/end users. Customers are an essential and useful source of
454 information on vulnerabilities observed or detected in the device.

455 **6.1.1.3 Third-party monitoring services**

456 If the manufacturer chooses to use an outside service to perform vulnerability monitoring, the contract should give a
457 clear description of what services are included. As appropriate, the contract should include details of the following:

458 — list of the affected products with specific version numbers;

459 — list of COTS and SOUP components with specific version numbers;

460 — list of the external sources other than the suppliers to be monitored;

461 — service level agreement on notifications (e.g. how promptly after the posting of a vulnerability are you
462 notified);

463 — if the contract includes testing of patches to COTS and SOUP components, agreements on what testing is
464 performed and how soon after notification (e.g. hotfixes to Windows, Adobe, Linux).

465 As a best practice, organizations that link newly identified vulnerabilities from national databases directly into change
466 requests in the associated product's tracking system to ensure they are assessed for possible risk.

#### 6.1.1.4 Product return and servicing

When the manufacturer receives a product for service, it should analyze the product's event logs for signs of intrusion and check the product for the presence of malware. This can be a valuable source of information on vulnerabilities in the device and help with revisions of the risk analysis for the product and with risk mitigation.

Care should be taken with returned product so that any malware present does not infect other devices or the environment in which it is being serviced. See Subclause 7.2, Secure disposal, for additional information about end of service returns.

#### 6.1.1.5 Changes in operational context

If the profile of the device is altered, whether consistent with or inconsistent with the instructions for use (IFU), the risk should be reassessed. Manufacturers may offer a service (or be requested) to check if the device is deployed as defined in the IFU and assess the risk.

A manufacturer should be familiar with the end user's operational context and workflow. If the security posture is dependent on specifics of a use environment, this should be made clear in the IFU, e.g., if the device can only be deployed on a private network with specific firewall protections.

Assessment of a new vulnerability by the manufacturer or by the HDO should include potential impact on the use environment. For example, a vulnerability could have little likelihood of exploit on a hospital network, but a high likelihood in home care use environments. This is an important part of the risk assessment of a vulnerability.

#### 6.1.1.6 Active monitoring

Another form of security monitoring is to actively monitor a device when it is in operation within an HDO's network. The most basic form of monitoring is security logging, which captures an electronic record of any security-related activity. It should be noted that if the security log is stored on the device itself, it is subject to tampering by a sophisticated attacker who wants to cover their tracks. Most security logging systems have the ability to securely transmit log data to a separate server.

Logs can be stored for later forensic analysis or may be used as part of an active monitoring system, looking for evidence of intrusion in real-time. The capabilities of large HDOs can be different than those of smaller HDOs, so the design of the device may need to be flexible in terms of what is logged and whether it is sent off-device.

Manufacturers may also desire that this active logging data be sent back to them for analysis of patterns that might be indicative of additional controls needing to be implemented. Again, flexibility is recommended as the policies for allowing remote transmission of data out of an HDO's network may vary by HDO.

Security logging is addressed in more detail in Annex B.

### 6.1.2 Coordinated vulnerability disclosure

As noted in Subclause 3.2, a coordinated vulnerability disclosure (CVD) program should be part of the vulnerability intake process. A means to receive vulnerability reports should be published publicly so that external parties can report vulnerabilities and understand the manufacturer's CVD process. As part of this process, a manufacturer should outline the expected responsibilities on both sides of the process (i.e., the reporting entity and the receiving entity) so that each can manage those expectations and ensure proper communication. There are a variety of resources available to guide the development of this process. More information is available in the bibliography. At a minimum, the process should define the scope of products and services, responsibilities, intake mechanisms (e.g., form or website), expected timelines, and legal considerations.

It is important to define the scope of products and services that will be part of the CVD program. The manufacturer should include a list of exclusions that explicitly defines out-of-scope products and services such as products and services (e.g., a third-party website) owned or hosted by third parties. Responsibilities for the CVD program should be well defined before launch of the program to assist with the efficiency of vulnerability intake and processing. Assignment of responsibilities should include, at a minimum, executive sponsorship, program management, and vulnerability analysts/validators. Executive sponsorship is advisable so that the program has support and funding from the manufacturer's leaders. Program management should be responsible for overseeing vulnerability analysis and validating that vulnerability intake and validation is performed in accordance with the manufacturer's procedures and policies. Vulnerability analysts and validators are responsible for day-to-day operations such as vulnerability intake, communications with the reporter of the vulnerability, vulnerability validation, and communications with product or service stakeholders that are negatively affected by the identified and validated vulnerability.

An intake medium such as an online form, website, or email address, should be provided for the reporting of vulnerabilities by the public. Robust security should be employed for the vulnerability intake medium as reported

vulnerabilities can have a drastic effect on the operation of the vulnerable product or service. CVD program stakeholders should develop an initial list of frequently asked questions and answers to inform the public of program rules and procedures. As the CVD program matures, the list should be periodically updated with frequently asked questions and answers to reduce the strain on the manufacturer's customer service department. The CVD program should also be properly coordinated and connected to the intake mechanism for other medical device complaints. Many customers are familiar with this established communication process and there should be a process for identifying security-related complaints so that they can be routed to the appropriate experts that are tied into the vulnerability analysis and correction process that addresses those vulnerabilities received from the CVD program.

#### 6.1.3 Bug bounty program

A growing issue for many manufacturers is the sale of identified vulnerabilities on black market websites for monetary gain. The common solution for many manufacturers has been the establishment of a bug bounty program. A bug bounty program will issue the reporter of a vulnerability a financial sum dependent on the product or service that the vulnerability effects and the severity of the vulnerability. A bug bounty program should define qualifying and non-qualifying vulnerabilities and include the requirements mentioned above. Applicable due diligence should be conducted to establish funding and resources before offering a bug bounty program.

It has also been noted that bug bounty programs are most effective for manufacturers that already have a mature SDLC program in place. If the manufacturer has not designed the device for security then a bug bounty program could create an excessive volume of reports, which would otherwise have been found in design controls. A bug bounty program is a good final check on manufacturers that believe they have achieved security maturity, not as a way to have researchers test the product to security maturity.

#### 6.1.4 Medical device cybersecurity signal handling and response

As discussed in Subclause 6.1.1, information pertaining to new threats, vulnerabilities, and knowledge should be collected from several sources. 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 an 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, disclosure of proprietary information, illegal access, misuse, or escalation of authorized access. Security incidents are discussed later in this document.

Cybersecurity signal handling starts with monitoring many sources for potential threat events: customer feedback, complaints, vendor reports, news items, etc. At its core, cybersecurity signal monitoring is about actively seeking information on the entire cybersecurity landscape of a product, while providing valuable insight needed to make risk mitigation decisions. Various cybersecurity signals can occur at any given time. Signals that can impact security risk assessments include, but are not limited to,

- a report of a security vulnerability from a third party;
- new threats and vulnerabilities detected through threat intelligence;
- customer questions regarding the security of the device;
- vulnerabilities detected internally by the manufacturer or product team.

An overview of the cybersecurity signal handling process recommended in this document is illustrated in Figure 2.

(next page)

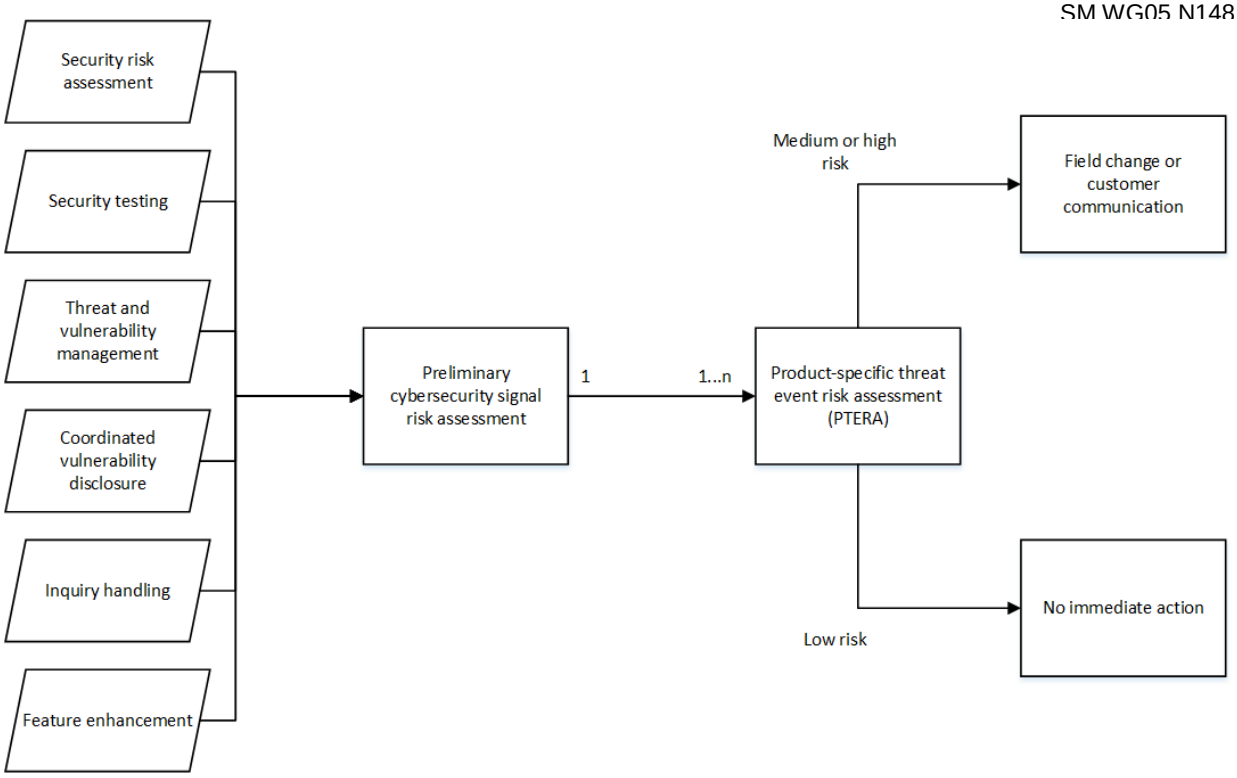


**Figure 2 — Cybersecurity signal handling process**

562

563 The cybersecurity signal handling process should capture relevant information and provide traceability from intake
564 through resolution. Information about a cybersecurity signal should be captured and documented at each phase
565 including the origin, date, time of the signal, technical information about the details of the event, a preliminary
566 determination of priority and applicability to different products, a product-specific assessment of the risk represented
567 by the signal, whether the signal requires a modification to the product, and if modification is required, what action
568 was taken and linkage to the elements that provide objective evidence that the action was taken.

569 After the preliminary cybersecurity signal risk assessment is completed, each impacted product team should perform
570 a product-specific threat event risk assessment (PTERA).

571 NOTE The PTERA is a component of the overall security risk assessment for a product – typically, security risk assessments
572 include the consideration of multiple threat events.

573 **6.1.4.1 Preliminary cybersecurity signal risk assessment**

574 Qualified security personnel should evaluate cybersecurity signals to assess their priority and potential applicability to
575 fielded products. When a cybersecurity signal occurs, it should be evaluated for potential impact to fielded products.
576 The performance of a preliminary cybersecurity signal risk assessment will inform the urgency and subsequent post-
577 release security risk analysis. Potential impact and categorization of the signal is defined in Table 1.

578 **Table 1 — Prioritization of cybersecurity signals**

| Priority | Explanation |
|---|---|
| **High** | Those signals that<br>— have the potential of a direct and serious impact on health condition or safety of a patient including<br>• death,<br>• an injury or serious deterioration to a patient, user, or other person, including<br>▪ a life-threatening illness or injury,<br>▪ permanent impairment of a body function,<br>▪ permanent damage to a body structure, or<br>▪ a condition necessitating medical or surgical intervention to prevent permanent impairment of a body function or permanent damage to a body structure. |

| Priority | Explanation |
|---|---|
| | — have the potential for simultaneously affecting many devices together,<br>— have the potential to affect a large number of devices within or across institutions,<br>— represent an actual breach of the security of a medical device that causes<br>• malfunction or unavailability of the device,<br>• compromise of confidentiality of information managed by the device, or<br>• compromise of security of the institution. |
| **Medium** | Those signals that have the potential to compromise the integrity or function of a medical device, thereby leading to<br>— malfunction or unavailability of the device unlikely to lead to harm,<br>— compromise of information managed by the device, or<br>— compromise of security of the institution. |
| **Low** | Signals not classified as above two categories to be treated as minor. Such signals have limited or no impact with a non-significant potential to affect many users. These signals can result from<br>— false triggers in the associated medical devices or infrastructure,<br>— investigation or examination of the device or the information supplied with the device, or literature indicating factors that could lead to a non-significant impact, or<br>— a report of "concern" about the security of a medical device. |

#### 6.1.4.2 Product-specific threat event risk assessment

A product-specific threat event risk assessment involves a determination of risk with respect to a specific product and an appropriate action to take based on that risk. The assessment the product teams perform can result in a change to the product or potentially no change. If the threat event is assessed as medium or high risk, based on review of the preliminary cybersecurity signal risk assessment, then a field change or customer communication should occur. If it is determined that the threat event is low risk, then no immediate action is typically required. The assessment process is illustrated in Figure 3.

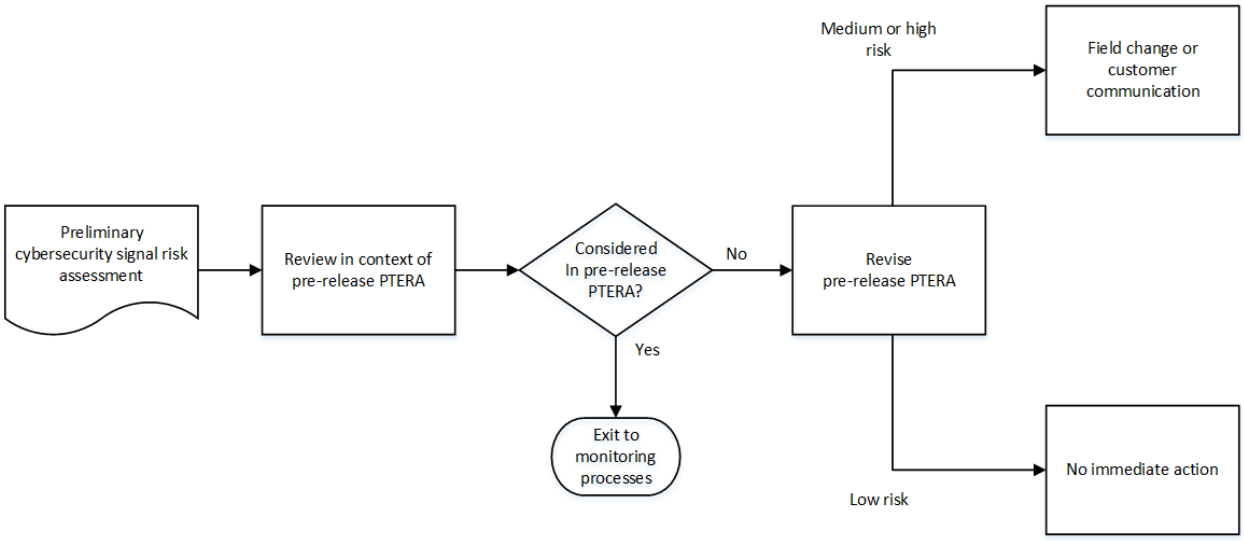


**Figure 3 — Product-specific threat event risk assessment**

When a cybersecurity signal is reviewed within the context of a pre-release PTERA (i.e., product-specific threat event risk assessment conducted prior to the fielding of the device), a determination is made as to whether the risk represented by the signal has been considered and included in the assessment.

If a determination is made that the cybersecurity signal represents a risk that was not previously considered, or the frequency of this and similar signals indicates that the likelihood was mischaracterized, then the security risk assessment should be revised. Figure 4 illustrates the overall process for a field change, showing that, over time, the security risk assessment is modified to reflect the dynamic nature of threats and vulnerabilities.

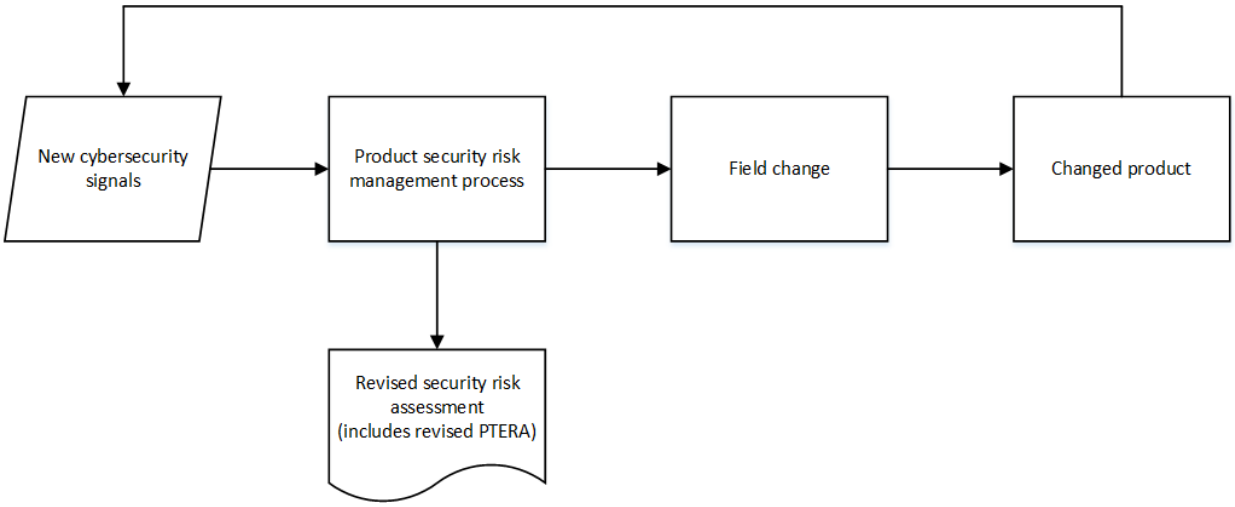


**Figure 4 — Field change and security risk assessment revision due to a new cybersecurity signal**

### 6.1.5 Medical device security incident handling and response

Incident handling and reporting should be an important part of a manufacturer's incident response plan. Security incidents can take several forms:

- incidents where harm has occurred;
- incidents where harm is likely if a device is compromised;
- active incidents where device infections are possible through shared vulnerabilities with other third-party platforms (e.g., WannaCry attack on vulnerable Windows systems);
- incidents where devices are not performing as expected but the evidence of the root cause being a security exploit has not been proven.

Device manufacturers should practice incident response through organizational “wargames” or “table-top exercises”. In such exercises, someone plans a series of events that unfold as an incident happens, and a set of stakeholders, ideally those specifically identified as the organization’s points-of-contact and decision makers for incident response, work together in a room to identify who they would communicate with and what information they would need as the event unfolds. Such practice, similar to a disaster response exercise for emergency service personnel, helps identify missing connections, and missing elements of the written incident response procedures. Repeating such exercises periodically with different scenarios helps hone the process and brings new players up to speed on what needs to be done.

#### 6.1.5.1 Security incident categories

A security incident can take many forms and it would be impractical for the manufacturer to develop procedures for all possible types of security incidents. Instead, it is useful to determine appropriate responses for common incident categories. Below is a list of common security incident categories:

- denial of service – an attack that prevents or impairs the authorized use of networks, devices, or applications by exhausting resources;
- malicious code – a virus, worm, trojan horse, or other code-based malicious entity that successfully infects a device;

- unauthorized access – a person or malicious process gains logical or physical access without permission to a network, device or, application;
- inappropriate usage – a person violates acceptable use of any network or computer policies;
- multiple component – a single incident that encompasses two or more incident categories.

Timely detection and notification of a security incident to affected personnel is crucial in reducing the impact of the security incident on the manufacturer or its customers. Security incident monitoring is reliant on people, process, and technology. People should be appropriately trained and knowledgeable on the identification of security incidents and how to handle and respond to security incidents once identified. Processes should be designed, developed, and implemented throughout the organization to facilitate consistent and effective security incident handling and response.

Lastly, technology should be deployed to detect threat events, assist in determining whether the threat event rises to the level of a security incident and support the handling of the security incident workflow and response. Technology solutions that can be implemented to identify threat events include, but are not limited to, anti-virus and anti-malware detection, governance, risk management, and compliance tools, host-based and network-based intrusion detection, and a security information and event management (SIEM) solution.

#### 6.1.5.2 Security incident assessment

A root cause analysis should be performed to determine if the problem is real and is related to cybersecurity. Personnel trained in the discipline and familiar with the product should be assigned to identify the source of the observed symptoms and determine their cause. Only when cause is established can the scope and severity of the problem be determined. Once triaging has occurred and validation has confirmed that a threat event is a security incident, the security incident handling process begins. As part of security incident handling, the incident first should be classified to determine an appropriate response. A non-exhaustive list of common security incident classification categories has been identified in the previous subclause. In addition to identifying the classification category, an assessment should occur to understand the level of risk associated with the security incident. This assessment can leverage the same criteria as defined previously for cybersecurity signals in Subclause 6.1.4.1.

When a security incident occurs and it is determined there is a potential for impact to patient safety (i.e., adverse event), it should be evaluated in accordance with the manufacturer's quality processes to determine the effect, if any, on patient safety and the predetermined quality and performance of any potentially affected products and product-impacting processes.

#### 6.1.5.3 Security incident response

Depending on the classification category and risk level, an incident response will be identified. High-risk security incidents will have the highest priority and should be addressed prior to other lower risk security incidents. In a scenario where there is more than one high-risk security incident, the incident response team will need to conduct an assessment to determine prioritization. Once high-risk security incidents are resolved, medium-risk security incidents will have the next level of priority. Similar to high- and medium-risk security incidents, if there are multiple low-risk incidents, the incident response team will need to conduct an assessment to determine prioritization.

It is important for the manufacturer to understand reporting requirements such as notifying organizational leadership, third-party stakeholders, regulators, law enforcement, and the public (including media). Organizational leadership should be notified immediately by the team that discovers, or receives credible information, that an incident has occurred. A list should be developed and maintained that outlines reporting requirements that need to be met during and post-incident.

Third-party stakeholders (e.g., customers) and regulators (e.g., the Food and Drug Administration (FDA)) should be notified per contractual and regulatory requirements, after a root cause has been determined, and after the incident has been managed. A manufacturer should identify and coordinate with local and federal law enforcement officials if the incident is the result of malicious activity perpetrated by a threat actor. Periodic communication is recommended to understand incident reporting channels where law enforcement involvement is required. Notifying the public (including media) is dependent upon local, national, and international laws. A manufacturer should identify their global footprint and should develop and actively maintain rationalized requirements for breach (incident) notification.

Complex manufacturers with multiple business units and corporate level security functions should develop communications and reporting functions so that the right points of contact are identified so when an incident is reported, communications paths to the affected business and up to senior management are already identified.

#### 6.1.6 Other sources of security performance information

Tracking security performance information for medical devices is a large undertaking. Manufacturers may have thousands of fielded devices across differing HDOs and home networks. As part of the manufacturer's vulnerability management program, key performance indicators should be captured to provide insight into the operations of the program. A few key performance indicators that should be considered for collection and reporting including, but are not limited to:

- percentage of the organization's fielded products that are currently undergoing active vulnerability monitoring;
- quantity of high and medium risk vulnerabilities for each product and more broadly each business unit;
- the time it takes to fix (or patch) a vulnerability in fielded devices can be recorded;
- the incident response time from initial identification to incident close out.

Many sources of security performance information exist from technical information to managerial information (e.g., cost). The manufacturer should conduct exercises with applicable stakeholders to identify security performance metrics that meet business needs.

### 6.2 Assessment

Any revision to the security risk assessment based on new information should be subject to the same level of control and review as the initial assessment. This would include any subsequent identification of risk control measures, if required. Such controls should include review and approval by individuals in the same functions or departments as those who signed off originally. Any new security-related observations are to be assessed using the current criteria for risk acceptability.

Figure 1 shows the basic flow for risk assessment when a new observation has been noted. If the observation is related to either safety or security, then it should be assessed against the current risk management file to determine if an update is required. ISO 14971 discusses the criteria for risk management file updates for new safety observations. For security observations, the risk management file will need updating if

- a new vulnerability has been publicly identified that changes estimates of the difficulty of attacking the device;
- a new type of attack emerges that improves the ability to exploit vulnerabilities that were previously assessed as not feasible;
- the observation includes direct evidence that the device has been successfully breached;
- compensating risk control measure is required;
- personally identifiable information (PII) from the device has been exposed outside the controlling organization (e.g. HDO); or
- a vulnerability has been shown that causes the device to become a pivot for attacking other connected devices and/or computing systems on a shared network.

The new residual risk level should be evaluated against the current risk acceptability criteria to determine if follow-up action is required. This action can take the form of

- a new safety control being required;
- a new security control being required; or
- only a security patch being required (a security patch has no effect on the device's essential performance, intended use or discernable change in the user interface requiring labeling updates).

In the two cases where new controls are to be introduced, they should be assessed to determine if they introduce new risks (e.g., new safety control impacts security or vice versa). If so, they should be assessed for necessary updates to the risk management file and the assessment process repeats.

#### 6.2.1 Assessing related products

When a new security risk assessment is performed for a device, the manufacturer should consider other devices, either fielded or in development, that might share the changed risk. If a new class of threat has been identified, or a

new class of attacks being used by a known threat type, this may also impact other devices that are exposed in a similar way. Those devices should be assessed as well.

If a new class of asset has been identified, other devices with similar assets should also be assessed to see if there are new or increased security risks requiring mitigation.

If a new vulnerability is identified, it can be from two different sources. One would be from third-party code (e.g. operating systems, common libraries). In that case, the manufacturer should review if other devices use the same third-party code that contains the same vulnerabilities. This is only tractable if the manufacturer creates an accurate bill of materials for components with potential security vulnerabilities (see Subclause 3.4)

The second source is if the vulnerability is discovered in software developed by the manufacturer, or by organizations directly contracted by the manufacturer to produce software to be incorporated into a device, then in addition to the review of whether that code is used in other devices, the manufacturer should consider whether the vulnerability is due to a common design or coding error. If so, this error might be repeated in other device software not directly shared with the initial device being assessed.

In such cases, the manufacturer should consider training to increase developer awareness of the impact of that coding error on device security and incorporate methods to examine for that type of coding error in future software review procedures. This can include incorporating rules into tools such as static code checkers to look for that coding error pattern.

#### 6.2.2 Speed of response

The overall assessment of risk (both safety and security) from the initial observation should be used to drive decision-making about the speed of the response. Manufacturers that produce devices on top of commercial operating systems and code libraries that require regular security patching from the sources of those items should consider creating a regular release schedule. In that case the speed decision is one of whether the update can wait and be part of the next scheduled release or if an off-cycle release is required.

Other issues that can impact the response speed decision include:

a) Are there compensating controls that can be implemented by the user while waiting for the patch to be released?

b) How effective would the communication of those compensating controls be? How quickly can a patch be deployed?

c) Does the vulnerability increase the likelihood of a compromised device becoming a pivot to attack other devices in the user's environment?

d) Will the update require regulatory pre-approval?

## 6.3 Action

Once a security incident has been evaluated and a decision is made to remediate any vulnerabilities, the manufacturer should take action to create a software update and communicate to all impacted stakeholders. This subclause provides recommendations on how to effectively conduct the activities around taking such action.

### 6.3.1 Internal coordination activities

#### 6.3.1.1 Internal stakeholders

Once a medical device security incident occurs, the responsible medical device manufacturer or their agents will need to coordinate internally their response to the incident. Prior to the incident, the manufacturer should proactively plan for coordination among affected internal stakeholders.

Internal stakeholders may vary based on the device's intended use and associated technologies used by the device. Some internal stakeholders are involved regardless of the device's intended use or associated technologies. Potential internal stakeholders that may be involved with internal coordination for a medical device security incident include:

— legal;

— medical;

— privacy;

— regulatory;

- compliance;
- research and development;
- product engineering;
- product risk management team;
- corporate communications;
- information technology (i.e., security and/or network);
- quality;
- customer relationship manager;
- incident coordinator;
- executive leadership;
- purchasing controls/supplier management.

#### 6.3.1.2 Deciding how to respond

Deciding how to respond to a medical device security incident is vital to a successful incident recovery outcome. Deciding how to respond should be operationalized in advance of an actual medical device security incident.

NIST SP 800-61 r2 Computer Security Incident Handling Guide identifies four phases of security incident handling:

a) preparation;

b) detection and analysis;

   Internal process intake with three vectors of internal communication development:

   1) internal;

   2) government;

   3) private entities/industry.

c) containment, eradication, and remediation;

d) post-incident activities.

NIST SP 800-61 r2 provides a framework of activities that should be established to create an incident response capability for an entity (such as a medical device manufacturer). NIST SP 800-61 r2 recommends:

a) creating an incident response policy and plan;

b) developing procedures for performing incident handling and reporting;

c) setting guidelines for communicating with outside parties regarding incidents;

d) selecting a team structure and staffing model;

e) establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies);

f) determining what services the incident response team should provide;

g) staffing and training the incident response team.

Deciding how to respond occurs during the observation and assessment phase of this life-cycle. Once an incident has been identified, the manufacturer's designated product security officer will assess and confirm whether the incident has potential impact to the manufacturer's medical device product(s). After confirmation of the incident, the manufacturer designated product security officer will contact the product incident response team (PIRT) governance team and the PIRT.

The PIRT should consist of representatives from those business functions that can rapidly respond and create the updates required at a speed consistent with the severity of the incident. This includes, but is not limited to

- research & development;
  - systems engineering;
  - software engineering;
  - hardware engineering.
- regulatory;
- quality;
- communications;
- manufacturing;
- customer support;
- sales & marketing.

The PIRT Governance Team should consist of leadership that can commit resources, and ensure that external communications and regulatory issues are managed according to company policy. This would include

- legal;
- regulatory;
- communications;
- quality;
- compliance;
- research & development leadership;
- senior leadership.

The PIRT will perform an analysis to determine if the manufacturer has means available to contain and eradicate the vulnerability associated with the incident. If the manufacturer can contain and eradicate the vulnerability, then that path will be followed. If the manufacturer cannot contain and eradicate the vulnerability, then the PIRT will report the vulnerability to a predetermined external information sharing analysis organization (ISAO) such as NH-ISAC and make mitigation recommendations to the external reporting entity (ISAO).

The designated product security officer and the PIRT should categorize the incident according to type and potential impact(s). The incident should then be classified and responded to in order of priority.

a) If immediate action is required, the designated information security officer will begin coordinated incident response activities.

b) If immediate action is not required, the designated product security officer will work with the reporting entity to determine appropriate response actions. In the case of multiple cybersecurity incidents occurring simultaneously, the designated product security officer and the PIRT will classify the incidents according to their immediate and potential adverse effects and prioritize recovery and investigation activities according to the severity of these effects.

#### 6.3.1.3 Internal coordination of external communications

NIST SP 800-61 r2 emphasizes the importance of organizations to work together during incident response. A key critical success factor for manufacturers is the advanced planning for coordinating internally any external communications that arise from the manufacturer's PIRT in response to the cybersecurity incident. PIRTs need to know, in advance, which cross-functional coordination should occur before any external communication is made. Having a communication plan to follow facilitates this process. A communication plan should determine

- the internal organizational units (stakeholders) are involved with external IRT communications (stakeholders may differ depending on criticality of the incident);
- the planned frequency of communications between internal stakeholders during the incident;
- how external PIRT communications will be internally approved and shared in advance with other internal organizational units;

- the means by which legal, public affairs, regulatory, product security and executive management are informed, and, if necessary, and the mechanism to formally approve the external communication;

  NOTE 1 Legal should be involved in any incident response activities/communications associated with law enforcement activities.

- who is authorized to speak about the incident to external stakeholders and the media;

- how corporate communications is to release the external communications through the appropriate internal channels.

  NOTE 2 Corporate communications is normally the appropriate internal channel for any external communications to the media. Corporate communications should be the internal organization responsible for handling any media inquiries.

PIRT training to prepare for handling internal coordination of external communications is important. Documentation via documented procedures and communication guidelines along with conducting table-top exercises in advance to confirm all parties know their roles and responsibilities is key as well. Training should include how situational awareness will be maintained by the PIRT and other affected stakeholders throughout the entirety of an incident response.

#### 6.3.1.4 Patch release coordination

Software updates/patch releases are part of the medical device software validation and risk analysis. Software updates (patches) due to cybersecurity concerns are necessary because they maintain a medical device's safety and effectiveness and are intended as mitigations to vulnerabilities. The manufacturer is responsible for patch approvals. Patch deployment is a shared responsibility between the manufacturer and, where applicable, HDOs and other affected patients and/or clients.

Based on the circumstances of the software update/patch, the manufacturer should review applicable regulatory guidance to determine whether the software update/patch requires regulatory notification.

Patch releases during a cybersecurity incident require cross functional coordination between the PIRT managing the incident and the product team responsible for the testing, verification, and validation of the patch. Items that require cross functional coordination include

- configuration management with the SBOM;
- notification of affected stakeholders about the patch release;
- all applicable device quality system and associated processes have been followed;
- timing of the patching deployment is understood by all affected stakeholders;
- software patches are code signed in such a way as to ensure the patch has not been altered.

#### 6.3.1.5 Incident response plan (impact and technical analysis)

The primary objective of a cybersecurity incident response plan is to manage a security incident in a way that limits damage, increases the confidence of external stakeholders, and reduces recovery time and costs. An additional objective is to improve efficiency and expedite response activities. Effective incident response plans

- improve decision-making;
- improve internal coordination;
- improve external coordination;
- establish clear roles and responsibilities across the manufacturer;
- limit damages by preventing further escalation of the incident.

The scalability of the incident response plan can range from a single organizational unit to an entire corporate enterprise.

Typical contents of a cybersecurity incident response plan should include

a) introduction (purpose, use, scope);

b) how to use the incident response plan (levels of incident response and escalation points);

c) event handling (event types, guides for categorization, suggested actions);

d) incident taxonomy (such as NIST taxonomy);

e) data-classification frameworks;

f) performance objectives (for data types and incident types);

g) definition of incident response team operating models;

h) activation of a war room or command center, thresholds for executives to take decisive measures, operating models such as documenting decision rights for who authorizes contacting law enforcement;

i) containment and investigation strategy (how to develop and implement);

j) communication plan (customers, media, regulators, and other stakeholders);

k) identification and remediation of failure modes (looking for ways the incident response could break down, then making enhancements under continuous improvement);

l) key tools for use during response;

m) response plans (plans for each incident type, checklists of key processes, actions, and notifications to be triggered in the event of a cyberattack, categorized by both incident and asset type);

n) post-incident procedures (evidence retention/evidence preservation strategy, lessons learned, continuous improvement opportunities).

#### 6.3.1.6 Executive communication plan

Another aspect of the incident response should be a clear understanding on when the executive committee of the company needs to be briefed on an on-going incident. Depending on the potential business risk associated with an incident, this can range from communications soon after the business impact is confirmed, or situations where the incident can be summarized after it has been resolved. It is important to define the risk threshold that drives the speed of communication before an incident occurs. This ensures that decisions can be made quickly, and responsible individuals can be trained. There could be thresholds where the executive committee will want to reach out to the board of directors for further communications and input.

#### 6.3.1.7 Tabletop exercise

Periodically, national groups like NH-ISAC will coordinate sector-wide national-level or regional-level tabletop exercises with the intent of performing simulated national-level cybersecurity incident management scenarios. Industry, regulators, ISAOs, and other cybersecurity related groups like ICS-CERT will jointly participate in these tabletop exercises. The knowledge gained from these tabletop exercises are funneled back to all the participants' organizations.

Typically, these tabletop exercises will provide an opportunity for various stakeholders to practice response and learn from others. Practice and shared experience are important elements of successful response plans. Those exercises that involve national-level scenarios and stakeholders provide the additional benefit of providing face-to-face interactions amongst the stakeholders who, otherwise, may interact only in the event of an emergency, which leaves little margin for error or delay.

As described elsewhere in this document, tabletop exercises also provide an important role in training and testing processes developed within an organization as part of their incident response plan.

### 6.3.2 Software maintenance

Medical devices may require software updates to address a potential defect or to add new functionality to a medical device. However, there are security considerations which need to be addressed when developing and deploying a software patch.

#### 6.3.2.1 Patch generation and distribution

Manufacturer should follow their SDLC to create and test a software update. Once an update has been developed, security protection mechanisms for authentication, integrity and confidentiality can be applied. These controls are generally additional steps in the build cycle.

The method for patch distribution can vary, but distribution should be automated to the greatest extent possible. Commonly used software update mechanisms include, but are not limited to: over-the-air (OTA) updates from device

manufacturer, updates delivered physically via storage media (e.g. USB), or updates delivered through the HDO network.

OTA updates are usually performed through the internet, where the software updates are hosted on a manufacturer-controlled webserver. The device connects to the internet to download the update. In absence of internet capable systems, manufacturers can deliver update through a physical storage media such as a universal serial bus (USB). In such a scenario, the dissemination of the storage media should be controlled strictly and utilize a dedicated removable storage media (e.g. USB memory sticks) to ensure that they are clean and malware-free. Regardless of the delivery mechanism used, the following important security aspects should always be considered in the distribution of software updates.

a) Software update mechanisms should verify the authenticity and integrity of a software patch prior to application.

   Integrity verification guards against improper information modification or destruction, and normally includes ensuring information non-repudiation and authenticity [15]. In practice, this means that any software patches are authorized patches that came from the manufacturer and that they have not been altered. Unauthorized patches or patches that have been modified can compromise the efficacy of the device and render it unsafe. They can also result in the unintentional compromise of the security of the medical device through the introduction of new, unknown vulnerabilities or the intentional compromise of the security of the medical device with malware. Integrity can normally be addressed with the use of cryptographic techniques such as code signing and hashed message authentication codes (HMACs)[1]. Use of integrity checks like cyclical redundancy codes and simple hashes are insufficient to protect against malicious modification.

b) Software update mechanisms could maintain the confidentiality of the software update contents.

   Contents of the software update could reveal sensitive information about medical device and how it works. For example, a third-party version of the database software in use. This information can potentially be used to an attacker's advantage. To protect the confidentiality of the software update, cryptographic solutions such as encryption can be used." to "If the contents of the software update reveals sensitive information about medical device and how it operates then the manufacturer should protect the confidentiality of the update using cryptographic solutions.

c) Software update mechanisms should employ an all or nothing installation.

   It is common for medical devices to consist of several different components of software, ranging from operating systems, to third-party libraries. If the medical device contains multiple software components, then an all or nothing updating mechanism would require that a user is unable to install portions of an update without installing all of it. For example, if a manufacturer released an update package that contained an update to the main medical device application and to a third-party library. Tthen the all or nothing mechanism would require that both updates be installed, or neither, and not allow a user to install only one. This addresses potential compatibility issues which could arise due to partial updates.

d) Software update mechanisms should enforce monotonicity.

   Monotonicity in software means prevention of a rollback, or prevention of downgrading a system to an older version. Rollbacks can result in malicious actors or uninformed users installing older, potentially more vulnerable version of software.

e) Software update mechanism should report back to the manufacturer verification of a successful installation.

   Having insight into what version of software updates a fielded system is running can provide a manufacturer with valuable information around software update adoption.

   Based on the device's communication capabilities there can be several ways to track delivery and installation of the updates. If the network configuration at the HDO allows this connectivity, the update mechanism should pass this information back to the manufacturer. If the device can wirelessly communicate to the manufacturer, then monitoring can be performed remotely with user's consent. Lastly, if the device cannot directly communicate with the manufacturer then another approach is to send out a survey to HDOs/clients/users.

[1] HMACs are difficult to secure because it requires a shared secret by the party creating the hash and the party verifying the hash. If the shared secret resides on the device then it may be compromised by an attacker, allowing the attacker to create patches that appear to be authentic and unmodified. Therefore, public key cryptographic techniques such as certificate-based digital signatures is preferred.

#### 6.3.2.2 Regulatory requirements

Manufacturers must adhere to region-specific regulations that govern how actions are reported.

For safe operation of the medical device, it is essential that the software updates are being installed regularly, and the device is working as intended post-installation. Based on the device's communication capabilities there can be several ways to track delivery and installation of the updates. If the device can communicate to the manufacturer, then monitoring can be performed remotely. If the device cannot directly communicate with the manufacturer then another approach is to send out a survey to HDOs/clients/users.

#### 6.3.2.3 Healthcare delivery organization control variations

Certain aspects of the HDO ecosystem might need to be taken into consideration while dispatching the updates. Such aspects include, but are not limited to: risk management policy of the HDO, support for various update delivery mechanisms, and HDO policy regarding software updates.

There can be several ways through which update delivery could be coordinated:

a) If OTA updates are delivered to the device from a manufacturer-controlled webserver, updates can be distributed in a push or pull mechanism. A push framework would force updates onto a medical device, this is not recommended due to the potential disruption of patient care it could cause. A pull framework would allow an HDO to update individual devices at a desired time.

b) If OTA updates are delivered from a manufacturer through an HDO controlled webserver and update distribution software. This additional software would provide the HDO control over distribution of the update within their network, and a location to see the current version of software on each system. Such a framework could, at the HDO's tasking, push the update to the medical devices when safe to do so.

c) Physical media installation would require the HDO to use physical means, such as a USB stick, to update devices one at a time.

### 6.3.3 External communication

Several types of communication paths should be outlined in a manufacturer's process when a new vulnerability is identified by a manufacturer. A process should be put in place to guide the types of communication that might be necessary, depending on the potential (or realized) severity and scope of impact.

**Table 2 — Types of external communication**

| Entity | Communication content | Purpose |
|---|---|---|
| Customer | Notifications of product field actions, recall activities, and other formal communication about impacts to products and related action | Communication with customers about security-related issues should be coordinated with existing regulated communication expectations and process. Some regional jurisdictions have security-specific guidelines, e.g. the United States. Specific considerations should be made regarding the routing of security-related notifications to customers since the people who require these types of notifications are often different than those receiving other recall and safety notifications. |

| Entity | Communication content | Purpose |
|---|---|---|
| Information Sharing and Analysis Organization (ISAO), such as NH-ISAC | Information about vulnerability<br>Affected products<br>Impact<br>Vulnerability characterization (e.g., exploitability, existence of exploit, difficulty)<br>Mitigation<br>Contact details | Vulnerability information should be disseminated so that impacted stakeholders can be notified. Also, for vulnerabilities identified in third-party software, sharing this information can help other manufacturers identify potential threats to products utilizing similar software in their products. |
| Government Cyber Emergency Response Organizations, such as ICS-CERT in the U.S. | Information about vulnerability<br>Affected products<br>Impact<br>Vulnerability characterization (e.g., exploitability, existence of exploit, difficulty)<br>Mitigation<br>Contact details | Vulnerability information should be disseminated so that impacted stakeholders can be notified. |
| Company website | A manufacturer may choose to publish detailed security advisories with content like that contained in ICS-CERT advisories.<br>Press releases regarding larger-scale global event responses and updates | The company website should serve as a specific point of contact and company position on certain security events as well as providing an efficient means of contact to appropriate staff within a manufacturer. |
| Government civil investigation entities such as FBI and DHS in U.S. | Manufacturers should identify their local branch and ensure they have the necessary contacts established should the need to initiate contact arise. | Government can assist in responding to global events with malicious intent, particularly if initiated by nation state. Assistance is also important if there is a need for criminal investigation. |
| Regulatory agencies | Manufactures should follow regulatory guidelines. | Regulatory compliance |

### 6.3.4 Interacting with healthcare delivery organizations

HDOs can have many communication venues that need to be notified when a security vulnerability is discovered. Both the biomedical engineering and the HDO security officer should be notified. Within the HDO there may need to be coordinated activity to contain or remediate a vulnerability by one or more organizations such as the biomedical engineering and/or the IT organization. When a manufacturer has learned that a vulnerability has caused a release of patient information or other sensitive organizational data, the privacy officer or other offices within the HDO may need to be notified.

### 6.3.5 Inventory management

Inventory management systems or asset tracking systems within the HDO can facilitate determining which medical devices are affected by the vulnerability and help prioritize the devices that need immediate attention. Capital equipment inventory can be another source within the HDO of medical devices to locate affected medical devices. Some vulnerabilities may need coordination between the HDO biomedical engineering departments, IT and/or the medical device manufacturer providing updates or remediation for the vulnerability.

## 7 Retirement/obsolescence

Figure 5 illustrates phases of the product life-cycle and associated support milestones including end of life (EOL) and end of support (EOS).

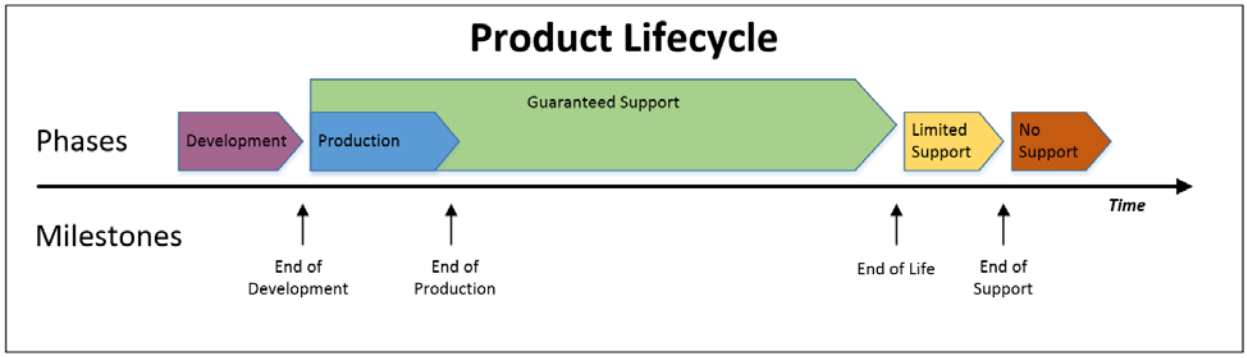


**Figure 5 — Product life-cycle and support milestones**

### 7.1 General considerations

Maintaining and supporting medical devices is a crucial function of a medical device manufacturer. Maintenance and support of hardware and software is dependent on several factors, including but not limited to

- hardware availability and driver support;
- 3rd party software support, including operating systems;
- compatibility issues between hardware and software components over time;
- technological advances in hardware and software.

Medical device manufacturers should take into consideration the support lifecycle of hardware and software components that comprise the medical device. To provide comprehensive support of a medical device, the manufacturer should be able to obtain support from the corresponding hardware and software vendors, by means of software/firmware updates and patches that address quality, performance, and security concerns.

Given the limited and finite lifecycle of hardware and software, manufacturers should define a support lifecycle that customers can reference that identifies how long the medical device will be supported and maintained with hardware, software and application software updates and patches. Support includes planned and unplanned maintenance activities in response to changes in the cyber threat landscape that could increase risk to the device.

As illustrated in Figure 5, support should be available until the product reaches the end of life (EOL) milestone. Support cannot be guaranteed beyond end of life. Manufacturers may be able to offer limited support or best effort support, depending upon the medical device until the end of support (EOS) date is reached. No support should be expected for any medical device past the established end of support milestone.

Manufacturers should communicate to customers and make public key dates that include how long to expect guaranteed support, when the device will reach end of life and end of support. Proactive communication is necessary to help customers plan for upgrades to supported devices. Communication should include the following:

a) Direct customer notification should be sent to the persons/distribution lists as identified by the customer and noted within their service record. Communication of approaching EOL and EOS dates should take place at least 18 months prior to these milestones. This notification should be sufficient to allow customers to plan for necessary updates and upgrades of medical devices prior to EOL and EOS.

b) Processes should be defined for updating customer contact information, customer records and medical device inventory status at least annually. This process should be documented in the sales terms and conditions. Accurate customer and install base information is necessary to ensure the timely and accurate dissemination of information to customers.

c) Public notifications should take place on the manufacturer's website and identify EOL and EOS milestones for each product as they are established and made available to customers. This type of notification often includes posting product specific information, including EOL and EOS dates on the manufacturer public Internet facing pages.

### 7.2 Secure disposal

Secure disposal is part of the security lifecycle for medical devices. Medical devices may need different processes for secure disposal depending on the type of device, manufacturer recommendations, or manufacturer requirements for end of medical device life processing or when the medical device requires service should provide Manufacturer recommended processes when the medical device is obsoleted or on replacing parts containing information that need secure disposal (e.g., hard drives, RAM).

The security risk management plan should describe plans for secure disposal and the device should be designed specifically to enable secure disposal. Service instructions should include a procedure for secure disposal and media security sanitization. MDMs should provide recommendations or processes for removing patient and organization data where storage media cannot be removed.

Secure disposal is specific to the type of storage media. Secure disposal of media includes shredding in-house, degaussing, or data removal by vendors specializing in secure disposal. See NIST 800-88 *Guideline for Media Sanitization* for additional information. Fixed location medical devices such as radiology equipment or other large medical devices which may contain hazardous materials should follow manufacturer recommendations for disposal. Medical devices may require return to the manufacturer or other contracted vendor for disposal. Manufacturer instructions should describe how the HDO may securely remove data from the medical device before return (e.g. hard drives or other storage device data should be removed from the medical device prior to shipping, but the MDM should not rely on the HDO properly doing so and should assume that the device has not had data securely removed until the manufacturer has verified there is no data.)

Equipment sent back to the manufacturer for disposal should be shipped using trusted carriers. Shipment should include tracking mechanisms to confirm where the device is located during the shipment process, and when it is received by the manufacturer. The service contact should contain language on carrier responsibilities for securing the device during shipment including requirements to notify the HDO if there are issues during shipping such as the device is lost or stolen.

Freestanding and mobile medical devices (e.g. pumps, monitors, and portable radiology devices) may be serviced by the HDO biomedical or contract service technicians when the devices are not returned to the manufacturer for disposal. As in the case of fixed location medical devices, MDM instructions should describe how the device may have data securely removed.

Where a storage media part is removed and not intended to be re-used, the HDO should securely destroy the storage media part, and where destruction is not feasible, securely remove any patient and organizational data residing on the storage media prior to disposal.

Where a medical device is decommissioned and disassembled so parts may be reused within the HDO, special care should be given storage media (e.g. hard drives, USBs, RAM/ROM). Storage media parts should be securely disposed or have patient and organizational data securely removed from the media prior to reuse. If the storage part is being inventoried by the HDO for reuse in another similar medical device, or will leave the HDO, the storage part should have any patient or organizational data securely removed from the device prior to inventory or reuse.

# Annex A
(Informative)

## Sample medical device security policy statements

This annex provides a non-exhaustive list of sample statements that can be incorporated in a manufacturer's medical device security policy.

NOTE Since these statements are not intended for use in the context of a standard or technical report, they do not follow the format prescribed by ISO Directives.

### A.1 Medical device security (top-level)

a) The organization has established and will maintain this Medical Device Security Policy to:

- Protect medical device associated information assets and supporting infrastructure from potential internal and external threats and hazards;
- Protect against reasonably anticipated unauthorized disclosures and uses of the medical device's sensitive information (e.g., patient health information, customer information, intellectual property);
- Protect against reasonably anticipated internal and external threats and hazards that may result in an impact to patient safety; and
- Maintain the confidentiality, integrity and availability of sensitive information stored, handled, or transmitted by the medical device.

b) The organization will establish, document, distribute and periodically review/update the Medical Device Security Policy and associated standards, and procedures to support maturity development and comply with applicable laws, statutory, regulatory, or contractual obligations, industry leading practices, organizational policies, and audit procedures.

c) The organization will implement medical device security roles, responsibilities, resources, tools, technologies, and processes needed for the successful implementation of this medical device security policy.

d) A Medical Device Security leader shall be appointed with the mission and resources to coordinate, develop, implement, and maintain the medical device security program that implements this policy.

e) The Medical Device Security Policy will be approved by company management, maintained and made available by management in accordance with business requirements and relevant laws and regulations.

f) Procedures will be established to review the Medical Device Security Policy at least annually, update it as needed, and make it available to all colleagues and individuals working on behalf of the organization.

g) A process for managing requests for policy exceptions will be established, documented, and made available.

h) Ad-hoc, supplemental medical device security requirements/guidance will be developed, approved, and communicated, as needed, between regular policy review/update cycles.

### A.2 Medical device security operations

a) Develop and implement a security risk management process that:

- Identifies medical device security requirements to be built into the design of new devices;
- Protects against all reasonably anticipated threats or hazards to the confidentiality, integrity and availability of the medical device and sensitive information;
- Manages security risk assessments and technical security testing, mitigation, acceptance, and reporting; and
- Controls security risks in third-party components.

b) Develop and implement a threat event and incident handling process that:

- Monitors industry sources for threat events, including third-party components and incidents and has processes in place to triage security.

c) Develop and implement a security education and training process that:

— Establishes and maintains a medical device security awareness program that communicates security requirements, industry trends, and other security-related topics to personnel responsible for managing the security of the organization's medical devices;

— Ensures that security personnel and individuals working on behalf of the organization are informed of their responsibilities to protect the confidentiality, integrity and availability of medical devices and sensitive information;

— Directs that security personnel and individuals working on behalf of the organization complete training within 90 days of hire and at least annually after hire; and

— Ensures that supplemental role-based training be provided to security personnel and individuals working on behalf of the organization who have a specific business need or whose duties involve designing, developing, or maintaining the organization's medical devices.

### A.3 Supporting security controls and implementation (by organizational function)

a) Access Control shall:

— Protect the confidentiality, integrity, and availability of the organization's medical devices by determining who can access different types of information, and by what means;

— Establish, maintain, document and review/update sufficient controls to restrict physical and logical access to sensitive information based on a need to know or least privilege basis (i.e., role-based access); and

— Implement physical, technical, and administrative safeguards to protect all forms of electronic media (e.g., laptops, CD-ROMs, USB drives, disks, tapes, etc.) containing sensitive information (e.g., patient data) from unauthorized access.

b) Human Resources shall:

— Work with the appropriate organization offices (e.g., Human Resources) to establish controls that ensure security personnel and individuals working on behalf of the organization are suitable for the roles for which they are placed and are trained on their information security responsibilities;

— Working with IT and other groups within the organization, define, document, and enforce security roles and responsibilities of security personnel and individuals working on behalf of the organization; and

— Establish, document, and review/update and enforce a formal disciplinary process for colleagues and individuals working on behalf of the organization who have violated information security policies and procedures.

c) Contracting and Outsourcing shall:

— Protect organization medical devices and information that is generated, accessed, stored, transmitted, processed or otherwise handled by external third parties.

— Establish and maintain a formal process for engaging and assessing the security practices (i.e., vendor risk) and security design and implementation (i.e., device risk) that is associated with third parties who provide services and or medical devices that the organization procures.

— Require contraction obligations for reporting and mitigating security vulnerabilities in products (e.g., software) or services.

— Terminate business with external third parties who collect, access, store, transmit, process or otherwise handle organization medical devices and information unless:

- The third-party security requirements are reviewed and approved by security staff.
- A contract is in place stating that the third party has implemented all appropriate administrative, physical, and technical safeguards.

d) Compliance shall:

— Ensure that the design, operation, use and management of medical devices adheres to applicable laws, statutory, regulatory or contractual obligations, and information security requirements;

— Establish and maintain a policy, standards, procedures, and guidance to ensure compliance with applicable laws, statutory, regulatory or contractual obligations, industry leading practices, and audit procedures; and

- Establish processes to address failure to comply with the Medical Device Security Policy and subsequent standards can result in disciplinary actions up to and including termination of employment for colleagues or terminations of contracts for contractors, partners, consultants, and other entities.
- Ensure that technical security requirements, appropriate to the nature of the device level of hazard and security risk, are established.

e) Asset and Information Management shall:

- Establish and maintain an asset management program to track medical device assets, assign ownership and responsibilities and associate medical device assets with threat and vulnerability information;
- Establish and maintain formal media sanitation policy for secure erasure of sensitive information; and
- Ensure that technical security requirements are enforced.

f) Business Continuity shall:

- Ensure that strategies and plans are in place to counteract interruptions to device operations and to protect critical device operational processes from the effects of major failures of system components or disasters and to ensure their timely resumption; and
- Establish and maintain a business continuity program to quickly resume device operational activities and recover information in the event of system failure or other disaster.

g) Systems Engineering shall:

- Establish and maintain a secure lifecycle design program that incorporates security into the device at the initial design and requirements stage; and
- Conduct risk assessments for legacy and discontinued devices, and implement extra security controls (e.g., segmentation) for devices that have reached end-of-life and are no longer supported.

# Annex B
(Informative)

# Security risk management for healthcare networks

## B.1 Healthcare network monitoring and device identification

Although much can be learned from monitoring traditional IT networks for cybersecurity risks, clinical networks risks are different from IT risks because of the need to ensure safety. The IT security industry has extensive experience at creating enterprise tools, but that industry is less familiar with safety critical networks. For this reason, HDOs traditionally use a risk-based approach to postmarket surveillance because of incidents where clinical engineers have accidentally impaired hospital operations with security tools designed for enterprise environments rather than clinical networks. For example, employing two-factor authentication as prescribed by the IT department may delay the application of timely care, or automatic application of patches to operating systems on devices without clinical evaluation of the changes can cause the device to operate differently than expected in a real environment.

In postmarket surveillance, HDOs commonly use both passive and active techniques to measure and assess populations of medical devices. Passive techniques include traffic flow analysis and device fingerprinting from broadcast/multicast traffic. Active techniques include management protocols, port scanning, and vulnerability scanning.

The advent of home healthcare and of smaller service-specific clinics means that devices are not always deployed in protected, IT-managed, networks. The management model of remote devices and even devices inside the HDO or clinic's network can vary in that the devices may be owned and managed by a third party, or even by the manufacturer.

### B.1.1 Operating environment

The manufacturer should also pay attention to the operating environment into which the device is to be deployed. To enumerate a few examples, a device can be deployed in any one of the following operating environments:

- fixed asset on a private hospital subnetwork;
- fixed asset on the hospital IT network;
- mobile asset on a private hospital subnetwork;
- mobile asset on the hospital IT network;
- fixed asset in a small clinic, without significant IT security expertise;
- mobile asset in a small clinic, without significant IT security expertise;
- fixed or mobile asset in a rudimentary home healthcare environment, with no IT support - this could include home dialysis and personal infusion pumps;
- asset without network connectivity in the normal course of events, e.g., an ambulance or simple Non-invasive Blood Pressure (NIBP) device in doctor's office;
- health software application running on a generic hardware platform.

### B.1.2 Design techniques to assist HDOs with device identification

HDOs struggle to identify all the devices on the network, particularly in the day of bring your own device (BYOD). Devices that are not deployed inside the hospital (e.g. home healthcare) should also be identified. For devices to be properly managed and monitored they need to be identifiable. The following design considerations for manufacturers may provide more effective device management for HDOs.

Techniques include:

a) When requesting an IP address via DHCP, include the Vendor Class option (option 60) in the DHCP request and put an unambiguous identifier in the Vendor Class field.

b) Devices use MAC addresses from a MAC range allocated to the manufacturer's organization (rather than a MAC range allocated to the HDO network interface's vendor). This makes it easier for many tools to identify the devices.

c) Support Network Access Control (NAC) on the device by implementing 802.1x as a supplicant.

d) When offering services via HTTP, include identifying strings in HTTP headers. Similarly, when offering other text-based services, include version numbers and make/model identifiers in header fields or text banners (greetings).

e) Respond to SNMP queries on the standard SNMP port (161). Especially, publish the system.sysName.0 and system.sysDescr.0 variables under the “public” community string.

f) Consider periodically sending beacons to announce the device’s identity. Such protocol options include the Link Layer Discovery Protocol (LLDP), Cisco Discovery Protocol (CDP) and Simple Service Discovery Protocol (SSDP).

g) Support TCP port scanning (e.g. Nmap) (both TCP SYN scanning and TCP connect scanning). Be aware that port scanning has been known to crash medical devices; the device should be thoroughly robust against this type of scanning. Test thoroughly with port scanners in the lab before release.

h) Support a Universally Unique Identifier (UUID); The device identifies itself using a UUID at startup, and/or on demand. IEEE 11073 SDC profile (OpenSDC) is based on Device Profile for Web Services (DPWS) which requires a UUID.

i) Ensure that every product line has an unambiguous name, and that each release of the product has a version identifier. Version identification is essential to management of patches and updates. If the version of the software cannot be reliably identified, and whether a patch has been applied or not, the patch process is not in control, and vulnerabilities cannot be reliably mitigated.

j) Design network protocols such that endpoints exchange version information. This would include the category of applications that authenticate using e.g. SSL/TLS.

k) Publish details about how to identify the version of a device by its network traffic.

Generic hardware platforms hosting health software applications should also identify themselves. In this case the hardware platform and application should both be identifiable. For example, the hardware platform could use the DHCP or NAC techniques, while the application identifies using HTTP strings or TLS. Ideally, there is a mechanism to correlate the application identifier to the host hardware identifier so they can be seen as a pair.

Alternatively, if the IT network assumes responsibility for hardware registration and verification, only the application may need to identify itself as a medical device.

In the following table maps these techniques according to their effort, their applicability to the operating environment, and the level of security assurance provided by the technique.

**Table B.1 — Identification techniques**

| | Identification technique | Manufacturer effort to implement | Operating environment (B.1.1) | Level of assurance |
|---|---|---|---|---|
| 1 | DHCP | low-medium | a, b, c, d | very low |
| 2 | MAC range management | low-medium | a, b, c, d, e, f, g | very low |
| 3 | NAC | medium | a, c, e, f | high (if credentialing)<br>medium otherwise |
| 4 | HTTP headers | low (if web server supported) | a, b, c, d, e, f, g, i | challenge resp./hash: medium<br><br>plaintext: low |
| 5 | SNMP | low (if SNMP already supported) | a, b, c, d, e, f, g | high if authenticated<br><br>low otherwise |
| 6 | LLDP | medium | a, b, c, d | low |
| 7 | Port scan | medium | a, b, c, d | low |

| | Identification technique | Manufacturer effort to implement | Operating environment (B.1.1) | Level of assurance |
|---|---|---|---|---|
| 8 | UUID | low | a, b, c, d, e, f, g, h, i | high if authenticated<br>low otherwise |
| 9 | Version identification | low | a, b, c, d, e, f, g, h, i | low |
| 10 | SW BOM | medium | a, b, c, d, i | medium |
| 11 | Network protocols | medium | a, b, c, d, e, f, g, i | high if authenticated<br>low otherwise |
| 12 | Network traffic profile | medium | a, b, c, d, i | medium |

### B.1.3 Asset identification

Whether the device security is managed as part of a HDO network, by the manufacturer, or as standalone device, the assets that are to be protected need to be identified. The manufacturer should provide a list of the assets contained in the medical device which are potentially in scope for and HDO that is monitoring the effectiveness of the security measures. This list of assets will help to determine the Security Information and Event Management (SIEM) monitoring that needs to be performed and the Events of Interest (EOI) that need to be detected and evaluated.

### B.1.4 Authorization servers

HDOs commonly use centralized authorization services such as Active Directory Domain Services. Tools such as these allow a device to offload the administration of authorization and role management and to allow use of standard IT tools for monitoring and logging authorization events.

### B.1.5 Structure of healthcare delivery organization networks

HDOs typically divide their host populations into at least three separate networks: clinical networks, general-purpose networks, and guest networks. Clinical networks typically include only those hosts on which clinical operations depend and these hosts are typically given highest priority in cases of congestion. Lowest priority goes to guest networks, which are typically given access to the Internet but not to any other internal networks. Desktop workstations and servers often appear on catch-all general-purpose networks. Any of these networks can be subdivided.

Clinical networks are often subdivided by modality, with functions such as surgical care and imaging using different (often segregated) networks. Security teams generally filter incoming and outgoing traffic flows to, from, and between these subnetworks to block all traffic not required for essential functions. Designers should expect devices to be placed on a subnetwork and should not depend on external services being reachable from devices. Designers should document their devices' typical network behavior so that HDOs can make appropriate changes to network configuration (e.g., firewall filtering rules).

#### B.1.5.1 Small clinic networks

Small clinics typically do not have the resources that a large HDO's IT department can deploy. It is unlikely that such an organization will have a mature security risk management process, sophisticated network analysis tools, or intrusion detection systems. They will often rely on the manufacturer to manage the security of the device and to provide details of vulnerabilities and of updates that need to be applied.

#### B.1.5.2 Home healthcare environments

End users in a home healthcare environment tend to be very trusting and willing to carry out steps communicated to them by an official sounding voice or email. It is unreasonable to expect these users to perform any configuration or maintenance tasks related to security. The device may not be remotely accessible, or it may be accessible through the end users Wi-Fi connection with rudimentary or no security in place. Monitoring and maintenance, if performed at all, are typically performed remotely.

## B.2 Security monitors and logging

NIST SP 800-64 indicates that "The ultimate objective of continuous monitoring is to determine if the security controls in the information system continue to be effective over time in light of the inevitable changes that occur in the system

as well as the environment in which the system operates". HDOs should not only monitor for undesirable events but also monitor the effectiveness of risk control measures. For example, monitoring the state of the firewall, responses to denial of service (DoS) attacks, and authentication events as a consequence of policies set.

A SANS Institute article "Successful SIEM and Log Management Strategies for Audit and Compliance" instructs "a single common denominator for all regulations requires that one log all events, and review them". In order to log events, the device needs to be monitoring assets and activities.

Design features that enable security monitoring and logging are essential to enabling security risk management on deployed devices. There are also industry compliance expectations that require an audit trail.

Service-oriented Architectures (SOA) present a slightly different challenge as many of the traditional tools (scanners, intrusion detection systems, etc.) are not as suitable for evaluating the security posture of a service-oriented architecture. NIST SP 800-94 "Guide to Intrusion Detection and Prevention Systems" provides detailed information on types of and uses for Intrusion detection systems. However, post-processing of security logs can be considered intrusion detection. More sophisticated users routinely apply machine intelligence to identify intrusions and exploits.

Data gathered as part of a monitoring effort can be used either real-time to generate security status information or as part of a periodic analysis or audit. Either way, essential feedback is given on the risk management in place. The nature of the data collected and the processing thereof will be influenced by privacy regulations. Care should be taken to anonymize all collected data.

### B.2.1 Passive monitoring

Passive device fingerprinting relies on identifiable device behaviors and often on correct use of network numbers. Device designers should assign devices MAC addresses from company-owned MAC range allocations, and they should include appropriate identifying strings when using network services such as mDNS or DHCP.

Once the assets of a device that require protection from security threats are identified, steps can be taken to monitor some of these assets, including:

- the performance of a device can be compromised by denial of service attacks or malware using device resources;

  NOTE Flow analysis, or "netflow," relies on special router features that announce network connections to a centralized collection point. HDOs often look for characteristic flows when trying to identify networked assets. Device designers should provide HDOs with documentation of the ports and external services the device expects to use.

- devices that can autonomously monitor CPU and memory usage and traffic patterns on interfaces;
- the creation, storage, transmission, or removal of PII on the device;
- administrative records, such as user profiles, authentication services, service records;
- review of monitoring logs.

Other tools used can include anti-virus applications.

Policy violations should be monitored. Actions to take when a policy is violated will depend on the policy, the severity of the violation, the intended use of the device, and the current state of the device; e.g. lockdown of the device may not be feasible if it is engaged in life-sustaining activities. All authentication events and data transfers should be monitored.

Periodic archiving and removal of PII is recommended. The device should monitor for the presence of PII, facilitate the cleanup activity, and monitor (i.e., log) the occurrence or absence of cleanup events, whether manual or automated.

The scope of the assets and data to be monitored should be chosen carefully, weighing the overhead and management of data against the usefulness of that data for predictive or post-event processing. Often it is not a single monitoring information source but rather the correlation of monitored data that indicates a security issue, and that facilitates locating the intrusion and the impacted assets. Further design considerations can include malware monitoring (including anti-virus engines) and intrusion detection. Intrusion detection tools are generally deployed at a network level rather than on the device itself.

It remains a design decision whether to include the correlation and interpretation of the data as an activity on the device to facilitate notifications, or whether to do it remotely using a SIEM system.

The scope of the monitoring performed and the analysis of the accumulated data will be heavily influenced by the deployment model, since logging large amounts of data on a device that is rarely connected will not be feasible. An architecture that supports prioritization of logged events, log rotation, and configurable logs is advisable when a device is to be deployed in varied environments.

The design should ensure that sufficient storage and bandwidth resources are available for the maintenance and transmission of the data that is generated from monitoring activities.

A well-formed device risk analysis will likely indicate what monitoring and logging features are required and desirable.

#### B.2.1.1 Technical recommendations for passive security logging

Essential to detecting threat events is a forensic, tamper-resistant security log. A potential way to achieve this is to implement an append-only log with authenticated chain of custody. Logging options include:

- a dedicated logging sink on the local network with device and system logs streaming to it in real time or "often" (e.g. every few minutes);

  NOTE This should include a built-in alert when logger cannot cope with load or is almost out of storage.

- an off-site logger with requirements similar to the local logging sink above, with a caching or contingency plan if external connection is unavailable;
- confidential (encrypted at-rest), tamper-evident and tamper-resistant hardware;
- meta-log for access to the logger and/or attempts to delete or alter information;
- authentication and authorization system for logger;
- a change tracking system with attribution and ability to revert.

Device manufacturers should consider a log interface exposed for log collection as distinct from collecting the logs (NIST SP 800-92). A "standardized" interface for frequent log export combined with a "black box"-type attachment for devices is recommended.

Log entries should have timestamps relative to the device rather than the network as the timing and sequence of events has meaning. Other techniques to consider with logging include:

- authoritative logger real-time clock;
- best practices: e.g. Vector clocks or other strong sequence-preserving techniques;
- independent timestamping of all messages by sender, preferably using an authoritative logger clock. If the sender has no real-time clock capabilities, a sequence number can be used.

Origin authentication, encryption, and validation of the log is recommended. If chain of custody is too onerous for a single device, it should still be considered for the network. In support of the authenticity of logs, the following may also be considered:

- tamper-evident and tamper-resistant hardware, including append-only logs;
- confidential (encrypted at-rest), authenticated (e.g., signed messages and Merkle trees for signature aggregation and bulk verification) storage;
- off-site backup using separate encryption and authentication keys, performed in near-real-time;
- meta-log for access to the logger and/or attempts to delete or alter information;
- authentication and authorization system for logger;
- change tracking system with attribution and ability to revert.

### B.1.1 Active monitoring

Active monitoring entails injecting test data or instructions to the device to ascertain the effectiveness of security controls. Consider it a controlled experiment where observed results can be compared to expected results. A common version of this is an application that simulates user activity. The user can be an expected user with a defined role (e.g., to determine that if role-based security measures are operating as expected) or an adversarial user (e.g.,

attempting a brute force password hacking attack or a DoS attack. Other tools used include port scanning, vulnerability scanning, and penetration testing.

HDOs, like any enterprise, routinely use port scanning to check for changes in the set of services that networked hosts are running. Manufacturers should port-scan their own devices under realistic network conditions to ensure that doing so does not trigger bugs or cause crashes. Popular open-source port scanners can be tuned for aggressiveness; designers should make sure to test the most aggressive settings.

Vulnerability scanners are also in common use. These software tools run a barrage of tests for known vulnerabilities. Device designers should already be using security scanners to test their own products during design phases, but frequent scanning during all phases of product development should minimize the chance of postmarket problems attributable to scanning.

These tools tend to be part of the IT network infrastructure and not usually included as a feature on the device.

### B.1.2 Security logs

NIST SP 800-92 “Guide to Security Log Management” provides a rich background on security logging including the types of logs, the challenges, and design and infrastructure issues associated with logging.

The SANS Consensus Policy Resource Community: Information Logging Standard document is a useful checklist for a designer attempting to decide what needs to be logged.

The data generated from these monitoring activities, often described as security logs, should be protected from tampering while at rest and during transmission. Other considerations include:

a) handling uncertainty in the log data;

— known unknowns;

When analyzing logged activity, do not ignore events of uncertain or unclear meaning. If there are log entries or events in the logs that cannot be identified or for which there is no coinciding incident (e.g. an exploit) or medical event, there may still be an issue, e.g., early indications of installation of malware that is not activated until months later. Retrieve and analyze the logs regularly to assure the correct operation of logging and the effectiveness of the filtering.

— unknown unknowns.

Periodically reevaluate what is being logged and what can be determined about your device or network from those logs. Regularly re-evaluate your rules or filters for the logs; Ensure that the data extracted from the logs matches explicit requirements for auditing or identification. Evaluate whether new rules or patterns need to be added based on known vulnerabilities or exploits.

b) device-only versus system interaction data;

Logs of systems or networks as well as individual device logs are a useful source of information for security monitoring, Post-processing of device and system logs can be cross-correlated to generate information on interactions and events that are not obvious at the device level. E.g. man-in-the middle attacks might be detected in this fashion. Institutions increasingly use machine-learning based tools to obviate the need for laborious manual correlation of all possible interactions.

c) security data retrieval and use environment.

While access to the logs or analytics may be well defined for large HDOs, smaller organizations may have fewer tools in place and fewer rules around access to logged data. Remote devices in a home healthcare environment or satellite clinics will still need to be monitored. It is important that the service agreement for the device includes provision for the security monitoring model. Post-processing may be the only option for remote devices.

The design should consider the means of access to the data. The solution will differ based on the network connectivity of the device, the model for processing the data, and the storage capabilities of the device. The device security logs may be kept on the device, sent periodically to a collection point (log server), or streamed to a log analyzer for real-time analysis.

Failsafes should exist for events that prevent the device from transmitting the logs upstream. For example, different categories of threat events can be defined, and retention of higher priority event logs prioritized over logs of lower category events.

Access to this data should be restricted to the appropriate roles. To facilitate this, and to comply with privacy rules, it is advisable that security logs remain independent of system and clinical logs, although there may be some events that fall into multiple logging categories. Logging features need to identify what logged data is for use by the end-user, and what is for use by Manufacturers. It is expected that the majority of security logs would be for the end-user, and manufacturer's logs would be limited to service or system logs. A feature that relies on the device "phoning home" in order to deliver logs to a manufacturer may not satisfy privacy or HDO IT-network rules and should not be relied upon.

Guides to security log management exist, albeit not specific to medical devices, for example:

a) NIST SP 800-92 Guide to Computer Security Log Management;

b) SANS Consensus Policy Resource Community: Information Logging Standard, 2014;

c) UL2800-0 DATA LOGGER and DATA STORE Requirements.

### B.2 Design pitfalls

Intrusion detection tools, and the countermeasures deployed, can have a detrimental effect on the intended use of the device. Tools and countermeasures should be carefully vetted for side-effects.

Prioritizing logging and monitoring to the detriment of intended use is also to be avoided. Logging and monitoring schemes should be designed such that they do not affect the intended use of the device, and are generally also not visible to the user of the device.

In the pursuit of greater security, manufacturers and integrators may be tempted to add multi-factor, role-based authorizations schemes. Authorization restrictions should not impair availability during intended use. The device architecture should support varying levels of role-based access where on-demand services are immediately accessible and others such as log retrieval are only accessible with the correct authorization.

# Annex C
(Informative)

## Establishing a coordinated vulnerability disclosure process

### C.1 Accepting vulnerability information from external sources

Medical device manufacturers should develop a robust vulnerability handling and coordinated disclosure processes to ensure that their products' residual risk is maintained at an acceptable level throughout the postmarket phase. Various procedural communicative and technical aspects of a well-designed process will assist in meeting this goal.

ISO/IEC 29147:2014 *Information Technology – Security Techniques – Vulnerability Disclosure* and ISO/IEC 30111:2013 *Information Technology – Security Techniques – Vulnerability Handling Processes* should be used by manufacturers as the basis for establishing their own vulnerability handling and responsible disclosure processes. Figure C.1 from ISO 29147:2014 provides a visual representation of how the two processes of vulnerability disclosure and vulnerability handling are tightly coupled:

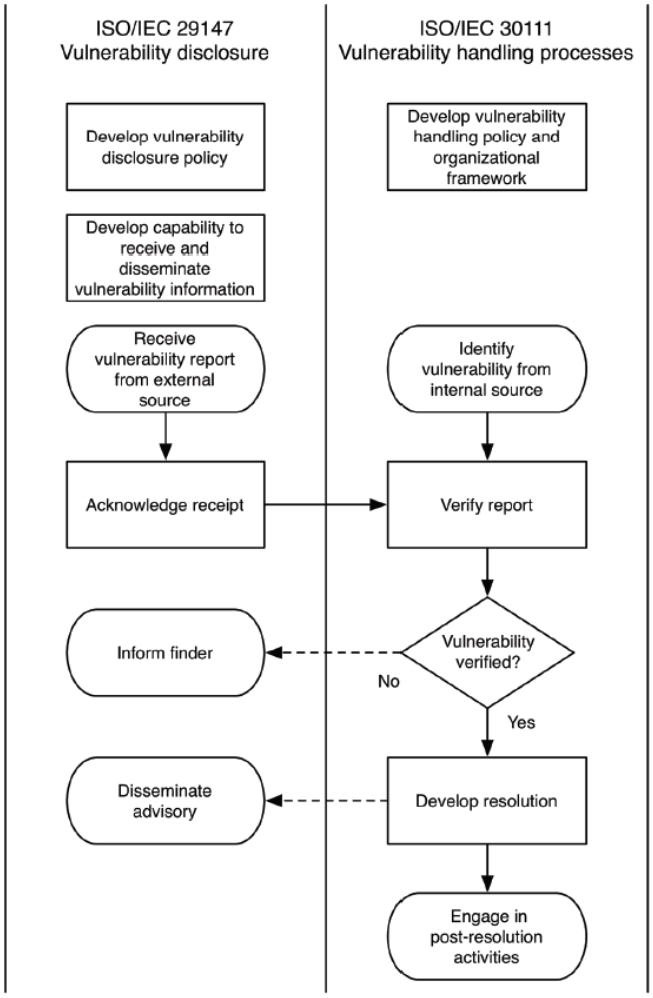


**Figure C.1 — A module of the interface between ISO/IEC 29147 and ISO/IEC 30111**

There are two key aspects of a successful vulnerability and responsible disclosure policy:

- established internal process for accepting vulnerability information received from external sources;
- established external and internal process for effectively communicating to the manufacturer's customers and users' important information regarding the recently disclosed known common vulnerability and exposures (KCVEs) pertaining to the manufacturer's medical device products.

### C.2 Accepting vulnerability information from external sources

In situations where an external source (e.g. security researcher) is attempting to establish contact with an appropriate information security representative from a manufacturer, it is important for the manufacturer's policy and external presence (e.g. web site) to be clear and explicit. The appropriate communication channel should be indicated, such as a dedicated group e-mail and telephone number as the most expeditious manner for the external source to contact the manufacturer and report the KCVE. Relying on generic customer support telephone numbers or email addresses is not optimal and may result in a possible excessive delay in responding. A KCVE notification directed to an employee not versed in security, or the request and source being transferred between multiple employees, or the request being lost before reaching the correct information security engineering representative could be catastrophic. In all of these examples, the external source reporting the KCVE could lose confidence in the manufacturer's process and possibly defer, out of frustration, to other another method such as a preemptive public disclosure. In these examples the manufacturer loses credibility and forgoes the opportunity to proactively confirm, verify and mitigate the potential cybersecurity and/or safety risk to patients.

Additionally, by having a streamlined responsible disclosure and vulnerability reporting process, this cybersecurity program maturity allows external reporting sources an opportunity to provide information on potentially unknown KVCEs and other product security vulnerabilities. The manufacturer should provide clear information to facilitate establishing a cooperative relationship with the KCVE reporting source always with the end goal of finding solutions that reduce the risks associated with a vulnerability.

Proactive and actionable activities should include

- direct communications channel to contact the manufacturer (with a secure option provided, such as PGP enabled e-mail);
- responsible disclosure and vulnerability reporting scope statement providing guidance of the goal of the disclosure process;
- details on the medical device information to be provided (e.g., product model, product serial number, configuration details, scenario to reproduce vulnerability);
- request for contact information for the reporting source – including phone numbers, e-mail address and PGP key;
- expected initial response time to the reporting source;
- specific steps the manufacturer is expected to perform with the information provided (e.g., attempt to reproduce);
- manufacturer's expectations on reporting source's actions (e.g. never perform test on medical devices in active or clinical use scenarios such as a hospital networked environment).

### C.3 Process for communicating to users and reporting known vulnerabilities

When a vulnerability is reported by an external source, the manufacturer should ensure the source is kept informed as appropriate on planned remediation efforts.

Once a remediation (e.g. compensating control, product update, software patch) is established, and successfully applied by the customer of the manufacturer, the final responsibility of a manufacturer's vulnerability disclosure process is to ensure that KCVE remediation information is disseminated as widely as possible. Depending on the vulnerability and the architected remediation, this process is divided into two main categories of actions; (1) customers, and (2) other governmental agencies (OGA). With regard to category (1), the list of parties to disclose to should include direct communication with patients, informing physicians, technical details being passed to HDO IT departments.

Within category (2), the KCVE details are written in the form of a KCVE narrative. The narrative is then reviewed with the US-Computer Emergency Response Team (US-CERT). US-CERT as part of the Department of Homeland Security (DHS) then will re-assign the proposed KCVE narrative to the Industrial Control System (ICS)-CERT. Once the approving authority, in the most general of cases, the ICS-CERT, located within the Idaho National Laboratory,

approves the agreed upon KCVE with the manufacturer, then the KCVE is released to the SECURE US-CERT Portal for secure access up to 30 days. After 30 days the US-CERT will release to the general public with a courtesy notification to the FDA.

Additional sources who could potentially report cybersecurity vulnerabilities to a manufacturer:

- threat information vendors;
- US-CERT;
- CVE-Details.com;
- MITRE CWE;
- MITRE CVE;
- NIST NCCoE;
- DHS;
- OGAs.

### C.4 Importance of third-party applications, firmware, and hardware

Another important aspect of a manufacturer's full lifecycle cybersecurity support for a product is to ensure that known common vulnerabilities and exposures that affect third-party software/hardware components are monitored and risk assessed. Medical devices have numerous third-party components which are all vulnerable to compromise. It is critically important that the KCVEs of these third-party applications, firmware, and hardware are also accounted for, tracked, and identified. Whenever possible, KCVEs should be remediated via software patch, firmware upgrade or appropriate compensating control.

Every manufacturer should have a robust process in place to identify the third-party components used in its products, track vulnerabilities against those components, access the impact of those vulnerabilities to the medical device, implement appropriate remediation(s), and communicate appropriate information on these details to customers. If common third-party components are used (e.g. operating systems), it is expected that many vulnerabilities will be reported to the larger IT community via platforms such as the National Vulnerability Database.

### C.5 U.S. FDA recognition of consensus standards (country-specific)

Irrespective of the originating source, a clear, consistent, and reproducible process for intake and handling of vulnerability information should be established and implemented by the manufacturer. FDA has recognized ISO/IEC 30111:2013 *Information Technology – Security Techniques – Vulnerability Handling Processes* that may be a useful resource for manufacturers.

Manufacturers should also adopt a coordinated vulnerability disclosure policy. FDA has recognized ISO/IEC 29147:2014 *Information Technology – Security Techniques – Vulnerability Disclosure* that may be a useful resource for manufacturers.

# 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

**Table D.1 — Mapping of defined terms**

| Defined terms - Postmarket Management of Cybersecurity in Medical Devices | ANSI/AAMI/ISO 14971:2007 | TIR97 |
|---|---|---|
| **A. Compensating Controls**<br>A cybersecurity compensating control is a safeguard or countermeasure deployed, in lieu of, or in the absence of controls designed in by a device manufacturer. (additional explanation follows) | The terms “compensating controls”, “safeguard”, and “countermeasure” are neither defined nor used in the document. Although “risk control measure” is not defined in clause 2, the term is used throughout the standard and in the definition of residual risk. | A compensating risk control measure is defined as a specific type of risk control measure:<br><br>**2.1**<br>**compensating risk control measure**<br>**compensating control**<br>specific type of risk control measure recommended by the device manufacturer in lieu of, or in the absence of, risk control measures implemented by the device manufacturer<br><br>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).<br><br>[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 recommended by the device manufacturer. Note 1 to entry has been added to delineate different types of measures.] |

| Defined terms - Postmarket Management of Cybersecurity in Medical Devices | ANSI/AAMI/ISO 14971:2007 | TIR97 |
|---|---|---|
| **B. Controlled Risk**<br>Controlled risk is present when there is sufficiently low (acceptable) residual risk of patient harm due to a device's particular cybersecurity vulnerability. | The term "controlled risk" is not defined or used in the document. Although "acceptable residual risk" is not defined in clause 2, the term is used in subclause A.2.6.2. The standard defines residual risk as:<br><br>**2.15**<br>**residual risk**<br>risk remaining after risk control measures have been taken<br><br>NOTE 1 Adapted from ISO/IEC Guide 51:1999, definition 3.9.<br><br>NOTE 2 ISO/IEC Guide 51:1999, definition 3.9 uses the term "protective measures" rather than "risk control measures." However, in the context of this International Standard, "protective measures" are only one option for controlling risk as described in 6.2. | The term "controlled risk" is not defined since it represents a state of acceptable residual risk for one type of harm ("patient harm") due to one type of hazard ("cybersecurity vulnerability").<br><br>The definition of residual risk is identical to the one incorporated in ISO 14971:2007 and AAMI TIR57:2016. |
| **C. Cybersecurity Routine Updates and Patches**<br>Cybersecurity "routine updates and patches" are changes to a device to increase device security and/or remediate only those vulnerabilities associated with controlled risk of patient harm. (additional explanation follows) | The term "cybersecurity routine updates and patches" is not defined or used in the document. Additionally, there are no instances of the terms "updates" and "patches" in the document. | The term "cybersecurity routine updates and patches" is not defined since it represents a specific type of risk control measure applied to a medical device that has acceptable residual risk for one type of harm ("patient harm").<br><br>The definition of residual risk is identical to the one incorporated in ISO 14971:2007 and AAMI TIR57:2016. |
| **D. Cybersecurity Signal**<br>A cybersecurity signal is any information which indicates the potential for, or confirmation of, a cybersecurity vulnerability or exploit that affects, or could affect a medical device. | The terms "cybersecurity signal" and "signal" are neither defined nor used in the document.<br><br>Clause 9 discusses several sources of information that are available during the production and post-production phase. | The definition of a cybersecurity signal is based on the FDA's postmarket guidance expanded to include threats and threat events:<br><br>**2.3**<br>**cybersecurity signal**<br>information that indicates the potential for, or confirmation of, a vulnerability, exploit, threat, or threat event that affects, or could affect a medical device<br><br>[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.] |

| Defined terms - Postmarket Management of Cybersecurity in Medical Devices | ANSI/AAMI/ISO 14971:2007 | TIR97 |
|---|---|---|
| **E. Exploit**<br>An exploit is an instance where a vulnerability or vulnerabilities have been exercised (accidently or intentionally) by a threat and could impact the safety or essential performance of a medical device or use a medical device as a vector to compromise a connected device or system. | The term "exploit" is not defined or used in the document. Annex E indicates "$P_2$ is the probability of a hazardous situation leading to harm." Similarly, an exploit does not necessarily lead to harm as recognized in the FDA's definition (i.e., "could impact").<br><br>The standard defines a "hazardous situation" as:<br><br>**2.4**<br>**hazardous situation**<br>circumstance in which people, property, or the environment are exposed to one or more hazard(s)<br><br>[ISO/IEC Guide 51:1999, definition 3.6]<br><br>NOTE See Annex E for an explanation of the relationship between "hazard" and "hazardous situation". | The definition of an exploit is based on the FDA's postmarket guidance but does not include the potential impact on safety or essential performance:<br><br>**2.6**<br>**exploit**<br>instance where a vulnerability or vulnerabilities have been exercised (accidently or intentionally) by a threat<br><br>[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.] |
| **F. Patient Harm**<br>Patient harm is defined as physical injury or damage to the health of patients, including death. | The document includes several instances of "patient harm" but the term is not defined. The definition of "harm" includes "damage to property or environment":<br><br>**2.2**<br>**harm**<br>physical injury or damage to the health of people, or damage to property or the environment<br><br>[ISO/IEC Guide 51:1999, definition 3.3] | The definition of "harm" is identical to the one used in AAMI TIR57:2016:<br><br>**2.11**<br>**harm**<br>physical injury or damage to the health of people, or damage to property or the environment, or reduction in effectiveness, or breach of data and systems security<br><br>[SOURCE: IEC 80001-1:2010, definition 2.8] |
| **G. Remediation**<br>Remediation is any action(s) taken to reduce an uncontrolled risk of patient harm posed by a device cybersecurity vulnerability to an acceptable level. | The term "remediation" is not defined or used in the document.<br><br>The standard does not distinguish between action(s) taken when the device is in an "acceptable residual risk" state vs. those applied when the device is in an "unacceptable residual risk" state. In both cases, the term "risk control measure" is used to describe the course of action. | The term "remediation" is not defined since it is the act of applying a risk control measure to a medical device that has unacceptable residual risk for one type of harm ("patient harm") due to one type of hazard ("cybersecurity vulnerability").<br><br>The definition of residual risk is identical to the one incorporated in ISO 14971:2007 and AAMI TIR57:2016. |

| Defined terms - Postmarket Management of Cybersecurity in Medical Devices | ANSI/AAMI/ISO 14971:2007 | TIR97 |
|---|---|---|
| **H. Threat**<br>Threat is any circumstance or event with the potential to adversely impact the device, organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.[18] | The term "threat" is not defined or used in the document. | The definition of "threat" is identical to the one incorporated in AAMI TIR57:2016:<br><br>**2.28**<br>**threat**<br>any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service<br><br>NOTE 1 to entry: Identical to NIST definition (SP 800-53) with the phrase "or the Nation" redacted.<br><br>[SOURCE: SP 800-53; SP 800-53A; SP 800-27; SP 800-60; SP 800-37; CNSSI-4009] |
| **I. Threat modeling**<br>Threat modeling is a methodology for optimizing Network/Application/Internet Security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system.[19] | The term "threat modeling" is not defined or used in the document. | Threat modeling is briefly discussed, but not defined, in TIR57 and should be initiated in the premarket phase. In the postmarket phase, a manufacturer should revise premarket threat models based on postmarket signals. This term is not defined in TIR97. |
| **J. Uncontrolled Risk**<br>Uncontrolled risk is present when there is unacceptable residual risk of patient harm due to inadequate compensating controls and risk mitigations. | The term "uncontrolled risk" is not defined or used in the document. The terms "mitigation" and "mitigations" are not used in the document. | The term "uncontrolled risk" is not defined since it represents a state of unacceptable residual risk for one type of harm ("patient harm") due to two types of hazards ("inadequate compensating controls and risk mitigations").<br><br>The definition of residual risk is identical to the one incorporated in ISO 14971:2007 and AAMI TIR57:2016. |

| Defined terms - Postmarket Management of Cybersecurity in Medical Devices | ANSI/AAMI/ISO 14971:2007 | TIR97 |
|---|---|---|
| **K. Vulnerability**<br>A vulnerability is a weakness in an information system, system security procedures, internal controls, human behavior, or implementation that could be exploited by a threat. | The term “vulnerability” is not defined or used in the document. | Annex A of AAMI TIR57:2016 explains a “vulnerability” is generally considered to be a specific type of hazard. The definition of “vulnerability” is identical to the one used in AAMI TIR57:2016:<br><br>**2.34**<br>**vulnerability**<br>weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source<br><br>[SOURCE: SP 800-53; SP 800-53A; SP 800-37; SP 800-60; SP 800-115; FIPS 200] |

1605

## Bibliography


[1] ANSI/AAMI/ISO 14971:2007, *Medical devices - Application of risk management to medical devices*. Association for the Advancement of Medical Instrumentation; 2007. Arlington, VA.

[2] ANSI/AAMI/ISO TIR24971:2013, *Guidance on the application of ISO 14971*. Association for the Advancement of Medical Instrumentation; 2013. Arlington, VA.

[3] ANSI/AAMI/IEC 80001-1:2010, *Application of risk management for IT networks incorporating medical devices - Part 1: Roles, responsibilities and activities*. Association for the Advancement of Medical Instrumentation; 2010. Arlington, VA.

[4] AAMI/ANSI/IEC, TIR 80001-2-2:2012, *Application of risk management for IT networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls*. Association for the Advancement of Medical Instrumentation; 2012. Arlington, VA.

[5] FDA, *Postmarket Management of Cybersecurity in Medical Devices*. https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf (Accessed 06 February 2018)

[6] HIMMS/NEMA Manufacturer Disclosure Statement for Medical Device Security (MDS2). http://www.himss.org/resourcelibrary/MDS2

[7] IEC TR 80002-2-8:2016, *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 TR 80001-2-2*

[8] NIST SP 800-61 Rev. 2, *Computer Security Incident Handling Guide*

[9] NIST SP 800-64 Rev. 2, *Security Considerations in the System Development Life Cycle*

[10] NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*

[11] NIST SP 800-92, *Guide to Computer Security Log Management*

[12] NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Information Systems and Organizations*

[13] NIST SP 800-88 Rev. 1, *Guidelines for Media Sanitization*

[14] NIST SP 800-30 Rev. 1, *Guide for Conducting Risk Assessments*

[15] NIST NISTIR 7298, Rev. 2, *Glossary of Key Information Security Terms*, May 2013. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

[16] *SANS Consensus Policy Resource Community: Information Logging Standard*, 2014

[17] *Best Practices: Event Log Management for Security And Compliance Initiatives*. Ipswitch Inc. 2010 https://www.ipswitch.com/Ipswitch/media/Ipswitch/Documents/Resources/Whitepapers%20and%20eBooks/ELM_Security_WP.pdf?ext=.pdf

[18] "Successful SIEM and Log Management Strategies for Audit and Compliance"; SANS Institute, 2010