1 **AAMI CDV TIR97**

2 **Committee Draft for Comment**

3 AAMI Technical Information Report

4 **NOTE** - This document is still under study and subject to change.
5 It should not be used for reference purposes.
6
7
8
9

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

10
11
12
13
14
15
16

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

20 **Keywords:** medical device, information security, risk management, postmarket
21
22
23
24
25
26
27
28
29 **Association for the Advancement of Medical Instrumentation**
30 4301 N Fairfax Drive, Suite 301, Arlington VA 22203-1633
31 Phone 703/525-4890 Fax 703/276-0793 Internet www.aami.org
32
33

Contents ....Page

53 **Foreword**

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

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

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

65 Suggestions for improving this recommended practice are invited. Comments and suggested revisions should be sent
66 to Technical Programs, AAMI, 4301 N. Fairfax Drive, Suite 301, Arlington, VA 22203-1633.

67 NOTE   This foreword does not contain provisions of AAMI TIR97, *Principles for medical device security — Postmarket risk*
68 *management for device manufacturers* (AAMI TIR97:201x), but it does provide important information about the development and
69 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.]

159
160 **2.3**
161 **cybersecurity signal**
162 information that indicates the potential for, or confirmation of, a vulnerability, exploit, threat, or threat event that
163 affects, or could affect a medical device
164
165 [SOURCE: Guidance for Industry and Food and Drug Administration Staff, Postmarket Management of
166 Cybersecurity in Medical Devices (2016), modified – The first sentence of definition IV.D has been incorporated with
167 changes to add threat and threat event.]
168
169 **2.4**
170 **end of life**
171 **EOL**
172 life-cycle stage of a product starting when the manufacturer no longer sells the product or guarantees full support
173
174 Note 1 to entry: There can be some level of support available by the manufacturer, but without guarantee that the
175 medical device can be maintained to its original specification and performance.
176
177 **2.5**
178 **end of support**
179 **EOS**
180 life-cycle stage of a product starting when the manufacturer terminates all service support activities
181
182 Note 1 to entry: Service support contracts do not extend beyond this point. No service activities, paid repair, parts
183 delivery or help desk support should be provided after a product has reached end of support.
184
185 **2.6**
186 **exploit**
187 instance where a vulnerability or vulnerabilities have been exercised (accidently or intentionally) by a threat
188
189 [SOURCE: Guidance for Industry and Food and Drug Administration Staff, Postmarket Management of
190 Cybersecurity in Medical Devices (2016), modified – Definition IV.E has been changed to remove language pertaining
191 to potential impacts.]
192
193 **2.7**
194 **guaranteed support**
195 life-cycle stage of a product starting with customer availability in the post-production phase and ending when the
196 product reaches end of life
197
198 Note 1 to entry: Limited support can be available once a medical device reaches end of life depending upon the
199 manufacturer, medical device, and other factors.
200
201 **2.8**
202 **information sharing and analysis center**
203 **ISAC**
204 operational entities formed by critical infrastructure owners and operators to gather, analyze, appropriately sanitize,
205 and disseminate intelligence and information related to critical infrastructure
206
207 Note 1 to entry: ISACs provide 24/7 threat warning and incident reporting capabilities and have the ability to reach
208 and share information within their sectors, between sectors, and among government and private sector stakeholders.
209
210 Note 2 to entry: ISACs are the original ISAOs for the critical infrastructure sectors.
211
212 Note 3 to entry: Although ISACs are recognized as operational entities in the United States, similar organizations
213 exist in other countries.
214
215 [SOURCE: U.S. Department of Homeland Security, National Infrastructure Protection Plan 2013, modified – The
216 second sentence has been moved to a note (Note 1 to entry). Note 2 to entry and Note 3 to entry have been added
217 to clarify applicability. The source for Note 2 to entry is https://nhisac.org/nhisac-faq/.]
218

219 **2.9**
220 **information sharing and analysis organization**
221 **ISAO**
222 any formal or informal entity or collaboration created or employed by public or private sector organizations, for
223 purposes of gathering, analyzing, communicating, disclosing, or voluntarily disseminating information in order to
224 better understand security problems and interdependencies related to critical infrastructure and protected systems, so
225 as to ensure the availability, integrity, and reliability thereof
226
227 Note 1 to entry: An ISAO communicates or discloses critical infrastructure information to help prevent, detect,
228 mitigate, or recover from the effects of an interference, compromise, or an incapacitation problem related to critical
229 infrastructure or protected systems.
230
231 Note 2 to entry: An ISAO voluntarily disseminates critical infrastructure information to its members, local, and Federal
232 Governments, or any other entities that may be of assistance. Similar organizations exist in other countries.
233
234 [SOURCE: 6 U.S.C § 131 (5), modified – The definition has been developed from subparagraph (a) modified to
235 include progressive verbs of subparagraphs (b) and (c). Note 1 to entry and Note 2 to entry have been added to
236 summarize subparagraphs (b) and (c), respectively, and to clarify applicability.]
237
238 **2.10**
239 **intended use**
240 **intended purpose**
241 use for which a product, process or service is intended according to the specifications, instructions, and information
242 provided by the manufacturer
243
244 [SOURCE: ANSI/AAMI/ISO 14971:2007, definition 2.5]
245
246 **2.11**
247 **life-cycle**
248 all phases in the life of a medical device, from the initial conception to final decommissioning and disposal
249
250 [SOURCE: ANSI/AAMI/ISO 14971:2007, definition 2.7]
251
252 **2.12**
253 **post-production**
254 part of the life-cycle of the product after the design has been completed and the medical device has been
255 manufactured
256
257 EXAMPLES transportation, storage, installation, product use, maintenance, repair, product changes,
258 decommissioning and disposal.
259
260 Note 1 to entry: The post-production phase includes devices manufactured and placed in inventory as well as those
261 devices that have been shipped to customers and are subject to postmarket surveillance.
262
263 [SOURCE: ANSI/AAMI/ISO 14971:2007, definition 2.11, modified – Note 1 to entry has been added.]
264
265 **2.13**
266 **security incident**
267 a violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices
268
269 [SOURCE: NIST SP 800-61 Rev. 2 (2012), modified – The term "computer" has been removed from the definition
270 included in section 2.1.]
271
272 **3   Postmarket considerations for security policies and security program administration**

273 **3.1   Medical device security policy**

274 AAMI TIR57:2016 provides guidance on developing a medical device security policy in Subclause 3.2, Management
275 responsibilities. The medical device security policy should define the manufacturer's high-level goals and objectives.
276 The policy should conform to postmarket regulatory requirements and be supported by standards, procedures, work
277 instructions, and other artifacts as needed that address security risk management, threat event, incident handling,
278 and security education and training. In addition, the policy should facilitate consistent and effective external
279 communications, as well as allow for monitoring and improvement of the processes required by the policy.

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

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

285 **3.2   Coordinated vulnerability disclosure**

286 Manufacturers should develop a coordinated vulnerability disclosure process to provide security researchers and
287 others with a means to communicate device vulnerabilities to appropriate parties. The manufacturer should utilize
288 customer communication channels to enable customers and users to report potential vulnerabilities. At the discretion
289 of the manufacturer, vulnerabilities should be reported to an information sharing and analysis organization, which
290 could help stakeholders understand and mitigate potential widespread security risk.

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

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

296 **3.3   Information sharing**

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

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

310 Reporting vulnerabilities to an ISAO allows critical cyber information to be shared with other stakeholders, which can
311 prevent similar vulnerabilities from being exploited or additional cyber-attacks from occurring. This relationship is
312 mutual and, in return for sharing information, manufacturers should be given information and intelligence on
313 vulnerabilities and threats across multiple sectors.

314 **3.4   Communication of security attributes**

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

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

327 To facilitate timely response to detailed customer inquiries, manufacturers should describe the security properties of a
328 device in a standard, internal, format during the product generation/creation process. This information supports the
329 preparation of MDS2 forms for the product and can form the basis of standard responses to customer inquiries.
330 MDS2 forms should be made available to customers upon request, and updated forms should be released whenever
331 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

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

6   Postmarket management of fielded devices

388

389 When a medical device is in use, there are several sources of information through which a manufacturer can learn of
390 vulnerabilities in, and threats to, fielded devices. It is important to understand that vulnerabilities exist in practically
391 any software-controlled device. They can be present in the third-party party code that is used in the device (operating
392 system, networking libraries, frameworks, etc.) or in the code developed by the manufacturer. Discovery can come
393 from outside the manufacturer (researchers, suppliers, national databases) or from internal or contracted device
394 analysis and/or testing.

395 After a vulnerability or threat is identified, it should be assessed for the risk to which it can expose the device, either in
396 terms of safety and to the security of the device or to other systems on the network to which the device is connected.
397 Figure 1 extends Figure 4 from AAMI TIR57:2016 to add the postmarket decision-making that can trigger a
398 reassessment of either safety or security risk (or both) and the decision whether a vulnerability requires correction,
399 whether new threats are significant, and whether additional safety or security controls are required.

400
401
402
403
404
405
406
407
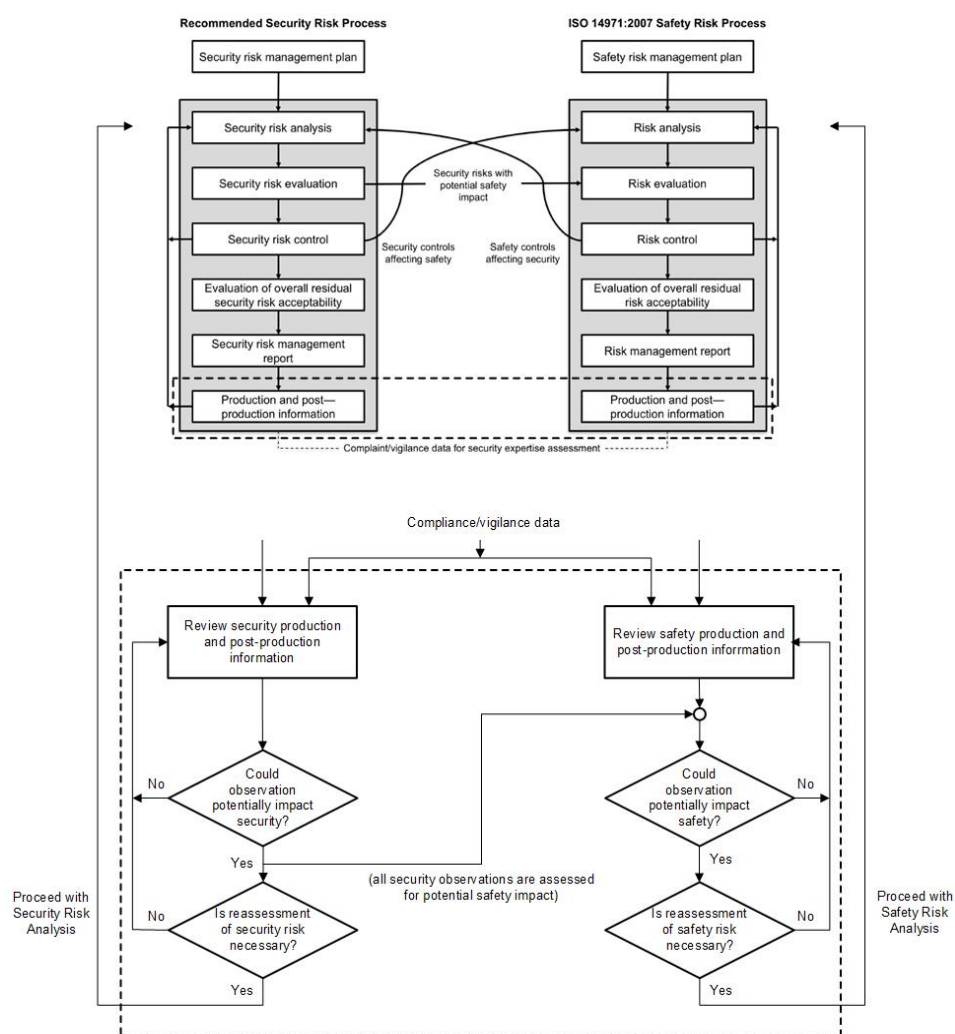408
409
410
411
412
413
414
415
416
417
418
419
420

Figure 1 — Postmarket decision-making flow diagram

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

424   —   observation and transmission;

425 — assessment; and

426 — action.

6.1 Observation and transmission

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.

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.

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.

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.

467 **6.1.1.4 Product return and servicing**

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

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

474 **6.1.1.5 Changes in operational context**

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

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

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

484 **6.1.1.6 Active monitoring**

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

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

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

496 Security logging is addressed in more detail in Annex B.

497 **6.1.2 Coordinated vulnerability disclosure**

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

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

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

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

527 6.1.3 Bug bounty program

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

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

539 6.1.4 Medical device cybersecurity signal handling and response

540 As discussed in Subclause 6.1.1, information pertaining to new threats, vulnerabilities, and knowledge should be
541 collected from several sources. Cybersecurity signals, as defined in Subclause 2.3, are a subset of "security
542 production and post-production information" as illustrated in Figure 1. Cybersecurity signals can impact security risk
543 assessments for multiple products. For each product-specific security risk assessment, a single cybersecurity signal
544 can impact assessments for multiple threat events.

545 Before categorizing an signal as a security incident, triaging should occur to validate that there has been an attempt
546 to access and/or adversely affect device data, systems, services, or networks in the context of data availability,
547 disclosure of proprietary information, illegal access, misuse, or escalation of authorized access. Security incidents are
548 discussed later in this document.

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

554 — a report of a security vulnerability from a third party;

555 — new threats and vulnerabilities detected through threat intelligence;

556 — customer questions regarding the security of the device;

557 — vulnerabilities detected internally by the manufacturer or product team.

558 An overview of the cybersecurity signal handling process recommended in this document is illustrated in Figure 2.
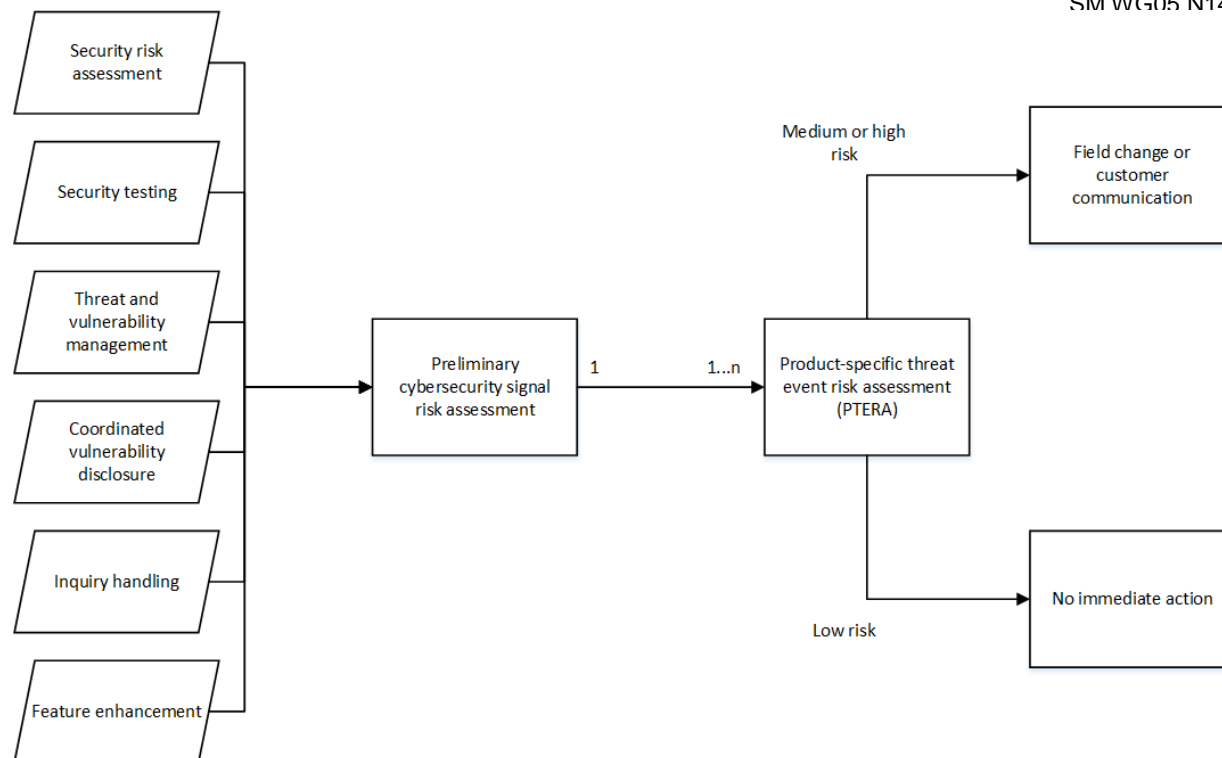
559

560

561 (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.

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
	— have the potential of a direct and serious impact on health condition or safety of a patient including
	  • death,
	  • an injury or serious deterioration to a patient, user, or other person, including
	    ▪ a life-threatening illness or injury,
	    ▪ permanent impairment of a body function,
	    ▪ permanent damage to a body structure, or
	    ▪ 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,
	— have the potential to affect a large number of devices within or across institutions,
	— represent an actual breach of the security of a medical device that causes
	   • malfunction or unavailability of the device,
	   • compromise of confidentiality of information managed by the device, or
	   • 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 — malfunction or unavailability of the device unlikely to lead to harm, — compromise of information managed by the device, or — 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 — false triggers in the associated medical devices or infrastructure, — 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 — a report of "concern" about the security of a medical device.

579

580 **6.1.4.2   Product-specific threat event risk assessment**

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

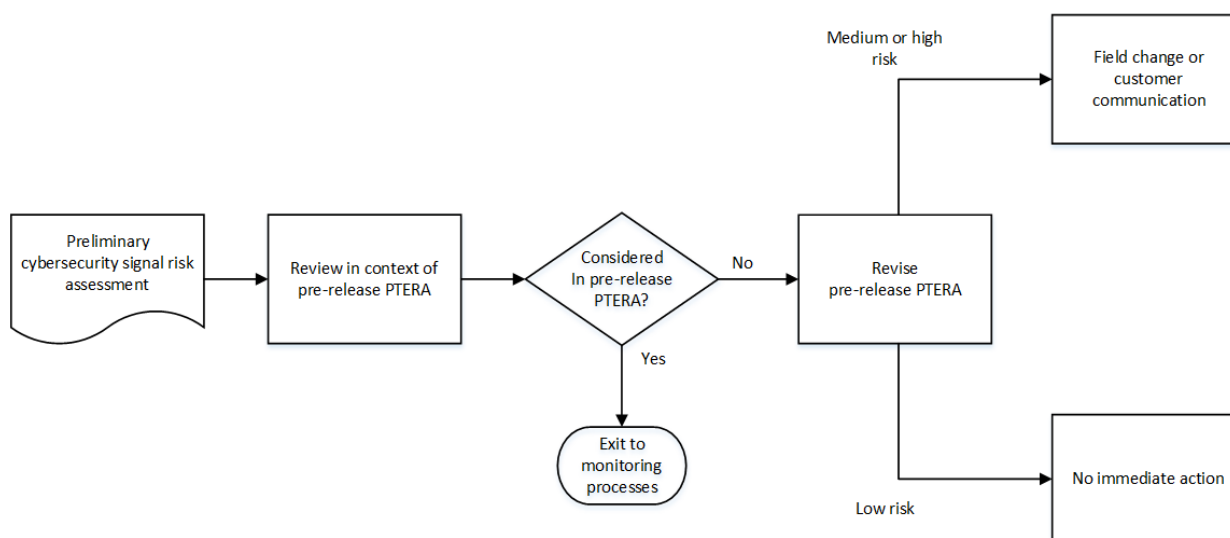587

588

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

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

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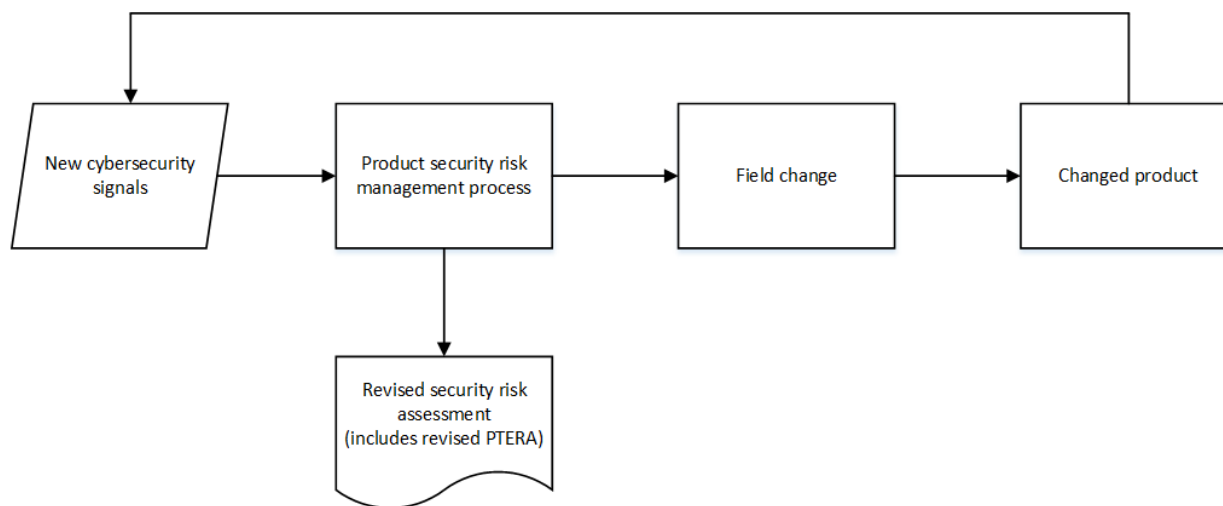596 security risk assessment is modified to reflect the dynamic nature of threats and vulnerabilities.

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

597

6.1.5 Medical device security incident handling and response

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

601 — incidents where harm has occurred;

602 — incidents where harm is likely if a device is compromised;

603 — active incidents where device infections are possible through shared vulnerabilities with other third-party
604 platforms (e.g., WannaCry attack on vulnerable Windows systems);

605 — incidents where devices are not performing as expected but the evidence of the root cause being a security
606 exploit has not been proven.

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

6.1.5.1 Security incident categories

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

619 — denial of service – an attack that prevents or impairs the authorized use of networks, devices, or applications
620 by exhausting resources;

621 — malicious code – a virus, worm, trojan horse, or other code-based malicious entity that successfully infects a
622 device;

623   — unauthorized access – a person or malicious process gains logical or physical access without permission to
624   a network, device or, application;

625   — inappropriate usage – a person violates acceptable use of any network or computer policies;

626   — multiple component – a single incident that encompasses two or more incident categories.

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

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

638 **6.1.5.2   Security incident assessment**

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

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

652 **6.1.5.3   Security incident response**

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

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

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

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

674 **6.1.6** **Other sources of security performance information**

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

680 — percentage of the organization's fielded products that are currently undergoing active vulnerability
681 monitoring;

682 — quantity of high and medium risk vulnerabilities for each product and more broadly each business unit;

683 — the time it takes to fix (or patch) a vulnerability in fielded devices can be recorded;

684 — the incident response time from initial identification to incident close out.

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

688 **6.2** **Assessment**

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

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

698 — a new vulnerability has been publicly identified that changes estimates of the difficulty of attacking the
699 device;

700 — a new type of attack emerges that improves the ability to exploit vulnerabilities that were previously
701 assessed as not feasible;

702 — the observation includes direct evidence that the device has been successfully breached;

703 — compensating risk control measure is required;

704 — personally identifiable information (PII) from the device has been exposed outside the controlling
705 organization (e.g. HDO); or

706 — a vulnerability has been shown that causes the device to become a pivot for attacking other connected
707 devices and/or computing systems on a shared network.

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

710 — a new safety control being required;

711 — a new security control being required; or

712 — only a security patch being required (a security patch has no effect on the device's essential performance,
713 intended use or discernable change in the user interface requiring labeling updates).

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

717 **6.2.1** **Assessing related products**

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

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

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

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

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

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

6.2.2 Speed of response

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

743 Other issues that can impact the response speed decision include:

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

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

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

750   d) Will the update require regulatory pre-approval?

6.3 Action

752 Once a security incident has been evaluated and a decision is made to remediate any vulnerabilities, the
753 manufacturer should take action to create a software update and communicate to all impacted stakeholders. This
754 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

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

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

763   — legal;

764   — medical;

765   — privacy;

766   — regulatory;

767   — compliance;

768   — research and development;

769   — product engineering;

770   — product risk management team;

771   — corporate communications;

772   — information technology (i.e., security and/or network);

773   — quality;

774   — customer relationship manager;

775   — incident coordinator;

776   — executive leadership;

777   — purchasing controls/supplier management.

778   **6.3.1.2 Deciding how to respond**

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

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

782   a)   preparation;

783   b)   detection and analysis;

784   Internal process intake with three vectors of internal communication development:

785   1)   internal;

786   2)   government;

787   3)   private entities/industry.

788   c)   containment, eradication, and remediation;

789   d)   post-incident activities.

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

792   a)   creating an incident response policy and plan;

793   b)   developing procedures for performing incident handling and reporting;

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

795   d)   selecting a team structure and staffing model;

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

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

799   g)   staffing and training the incident response team.

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

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

807 — research & development;

808 • systems engineering;

809 • software engineering;

810 • hardware engineering.

811 — regulatory;

812 — quality;

813 — communications;

814 — manufacturing;

815 — customer support;

816 — sales & marketing.

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

819 — legal;

820 — regulatory;

821 — communications;

822 — quality;

823 — compliance;

824 — research & development leadership;

825 — senior leadership.

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

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

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

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

840 **6.3.1.3 Internal coordination of external communications**

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

846 — the internal organizational units (stakeholders) are involved with external IRT communications (stakeholders
847   may differ depending on criticality of the incident);

848 — the planned frequency of communications between internal stakeholders during the incident;

849 — how external PIRT communications will be internally approved and shared in advance with other internal
850   organizational units;

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

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

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

856 — how corporate communications is to release the external communications through the appropriate internal
857   channels.

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

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

865 **6.3.1.4 Patch release coordination**

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

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

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

876 — configuration management with the SBOM;

877 — notification of affected stakeholders about the patch release;

878 — all applicable device quality system and associated processes have been followed;

879 — timing of the patching deployment is understood by all affected stakeholders;

880 — software patches are code signed in such a way as to ensure the patch has not been altered.

881 **6.3.1.5 Incident response plan (impact and technical analysis)**

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

885 — improve decision-making;

886 — improve internal coordination;

887 — improve external coordination;

888 — establish clear roles and responsibilities across the manufacturer;

889 — limit damages by preventing further escalation of the incident.

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

892 Typical contents of a cybersecurity incident response plan should include

893   a)   introduction (purpose, use, scope);

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

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

896   d)   incident taxonomy (such as NIST taxonomy);

897   e)   data-classification frameworks;

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

899   g)   definition of incident response team operating models;

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

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

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

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

906   l)   key tools for use during response;

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

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

911   **6.3.1.6   Executive communication plan**

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

919   **6.3.1.7   Tabletop exercise**

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

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

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

932   **6.3.2   Software maintenance**

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

936   **6.3.2.1   Patch generation and distribution**

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

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

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

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

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

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

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

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

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

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

977 d) Software update mechanisms should enforce monotonicity.

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

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

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

984 Based on the device's communication capabilities there can be several ways to track delivery and
985 installation of the updates. If the network configuration at the HDO allows this connectivity, the update
986 mechanism should pass this information back to the manufacturer. If the device can wirelessly
987 communicate to the manufacturer, then monitoring can be performed remotely with user's consent. Lastly, if
988 the device cannot directly communicate with the manufacturer then another approach is to send out a
989 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.

990 **6.3.2.2 Regulatory requirements**

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

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

997 **6.3.2.3 Healthcare delivery organization control variations**

998 Certain aspects of the HDO ecosystem might need to be taken into consideration while dispatching the updates.
999 Such aspects include, but are not limited to: risk management policy of the HDO, support for various update delivery
1000 mechanisms, and HDO policy regarding software updates.

1001 There can be several ways through which update delivery could be coordinated:

1002   a) If OTA updates are delivered to the device from a manufacturer-controlled webserver, updates can be
1003   distributed in a push or pull mechanism. A push framework would force updates onto a medical device, this
1004   is not recommended due to the potential disruption of patient care it could cause. A pull framework would
1005   allow an HDO to update individual devices at a desired time.

1006   b) If OTA updates are delivered from a manufacturer through an HDO controlled webserver and update
1007   distribution software. This additional software would provide the HDO control over distribution of the update
1008   within their network, and a location to see the current version of software on each system. Such a framework
1009   could, at the HDO's tasking, push the update to the medical devices when safe to do so.

1010   c) Physical media installation would require the HDO to use physical means, such as a USB stick, to update
1011   devices one at a time.

1012 **6.3.3 External communication**

1013 Several types of communication paths should be outlined in a manufacturer's process when a new vulnerability is
1014 identified by a manufacturer. A process should be put in place to guide the types of communication that might be
1015 necessary, depending on the potential (or realized) severity and scope of impact.

1016 **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 Affected products Impact Vulnerability characterization (e.g., exploitability, existence of exploit, difficulty) Mitigation 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 Affected products Impact Vulnerability characterization (e.g., exploitability, existence of exploit, difficulty) Mitigation 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. 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

1017

1018   **6.3.4**   **Interacting with healthcare delivery organizations**

1019   HDOs can have many communication venues that need to be notified when a security vulnerability is discovered.
1020   Both the biomedical engineering and the HDO security officer should be notified. Within the HDO there may need to
1021   be coordinated activity to contain or remediate a vulnerability by one or more organizations such as the biomedical
1022   engineering and/or the IT organization. When a manufacturer has learned that a vulnerability has caused a release of
1023   patient information or other sensitive organizational data, the privacy officer or other offices within the HDO may need
1024   to be notified.

1025 **6.3.5   Inventory management**

1026 Inventory management systems or asset tracking systems within the HDO can facilitate determining which medical
1027 devices are affected by the vulnerability and help prioritize the devices that need immediate attention. Capital
1028 equipment inventory can be another source within the HDO of medical devices to locate affected medical devices.
1029 Some vulnerabilities may need coordination between the HDO biomedical engineering departments, IT and/or the
1030 medical device manufacturer providing updates or remediation for the vulnerability.

1031 **7   Retirement/obsolescence**

1032 Figure 5 illustrates phases of the product life-cycle and associated support milestones including end of life (EOL) and
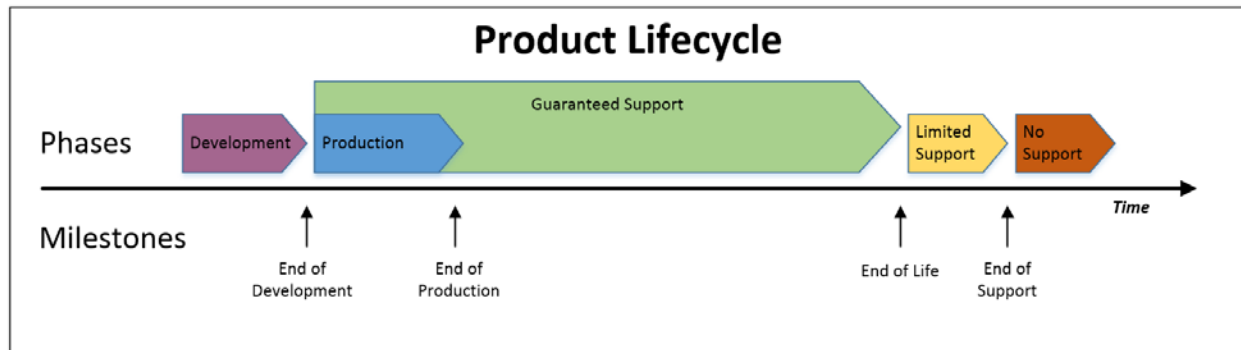1033 end of support (EOS).

1034

1035 **Figure 5 — Product life-cycle and support milestones**

1036 **7.1   General considerations**

1037 Maintaining and supporting medical devices is a crucial function of a medical device manufacturer. Maintenance and
1038 support of hardware and software is dependent on several factors, including but not limited to

1039 — hardware availability and driver support;

1040 — 3rd party software support, including operating systems;

1041 — compatibility issues between hardware and software components over time;

1042 — technological advances in hardware and software.

1043 Medical device manufacturers should take into consideration the support lifecycle of hardware and software
1044 components that comprise the medical device. To provide comprehensive support of a medical device, the
1045 manufacturer should be able to obtain support from the corresponding hardware and software vendors, by means of
1046 software/firmware updates and patches that address quality, performance, and security concerns.

1047 Given the limited and finite lifecycle of hardware and software, manufacturers should define a support lifecycle that
1048 customers can reference that identifies how long the medical device will be supported and maintained with hardware,
1049 software and application software updates and patches. Support includes planned and unplanned maintenance
1050 activities in response to changes in the cyber threat landscape that could increase risk to the device.

1051 As illustrated in Figure 5, support should be available until the product reaches the end of life (EOL) milestone.
1052 Support cannot be guaranteed beyond end of life. Manufacturers may be able to offer limited support or best effort
1053 support, depending upon the medical device until the end of support (EOS) date is reached. No support should be
1054 expected for any medical device past the established end of support milestone.

1055 Manufacturers should communicate to customers and make public key dates that include how long to expect
1056 guaranteed support, when the device will reach end of life and end of support. Proactive communication is necessary
1057 to help customers plan for upgrades to supported devices. Communication should include the following:

1058   a) Direct customer notification should be sent to the persons/distribution lists as identified by the customer and
1059   noted within their service record. Communication of approaching EOL and EOS dates should take place at
1060   least 18 months prior to these milestones. This notification should be sufficient to allow customers to plan
1061   for necessary updates and upgrades of medical devices prior to EOL and EOS.

1062   b)   Processes should be defined for updating customer contact information, customer records and medical
1063   device inventory status at least annually. This process should be documented in the sales terms and
1064   conditions. Accurate customer and install base information is necessary to ensure the timely and accurate
1065   dissemination of information to customers.

1066   c)   Public notifications should take place on the manufacturer's website and identify EOL and EOS milestones
1067   for each product as they are established and made available to customers. This type of notification often
1068   includes posting product specific information, including EOL and EOS dates on the manufacturer public
1069   Internet facing pages.

1070   **7.2   Secure disposal**

1071 Secure disposal is part of the security lifecycle for medical devices. Medical devices may need different processes
1072 for secure disposal depending on the type of device, manufacturer recommendations, or manufacturer requirements
1073 for end of medical device life processing or when the medical device requires service should provide Manufacturer
1074 recommended processes when the medical device is obsoleted or on replacing parts containing information that need
1075 secure disposal (e.g., hard drives, RAM).

1076 The security risk management plan should describe plans for secure disposal and the device should be designed
1077 specifically to enable secure disposal. Service instructions should include a procedure for secure disposal and media
1078 security sanitization. MDMs should provide recommendations or processes for removing patient and organization
1079 data where storage media cannot be removed.

1080 Secure disposal is specific to the type of storage media. Secure disposal of media includes shredding in-house,
1081 degaussing, or data removal by vendors specializing in secure disposal. See NIST 800-88 *Guideline for Media*
1082 *Sanitization* for additional information. Fixed location medical devices such as radiology equipment or other large
1083 medical devices which may contain hazardous materials should follow manufacturer recommendations for disposal.
1084 Medical devices may require return to the manufacturer or other contracted vendor for disposal. Manufacturer
1085 instructions should describe how the HDO may securely remove data from the medical device before return (e.g.
1086 hard drives or other storage device data should be removed from the medical device prior to shipping, but the MDM
1087 should not rely on the HDO properly doing so and should assume that the device has not had data securely removed
1088 until the manufacturer has verified there is no data.)

1089 Equipment sent back to the manufacturer for disposal should be shipped using trusted carriers. Shipment should
1090 include tracking mechanisms to confirm where the device is located during the shipment process, and when it is
1091 received by the manufacturer. The service contact should contain language on carrier responsibilities for securing the
1092 device during shipment including requirements to notify the HDO if there are issues during shipping such as the
1093 device is lost or stolen.

1094 Freestanding and mobile medical devices (e.g. pumps, monitors, and portable radiology devices) may be serviced by
1095 the HDO biomedical or contract service technicians when the devices are not returned to the manufacturer for
1096 disposal. As in the case of fixed location medical devices, MDM instructions should describe how the device may
1097 have data securely removed.

1098 Where a storage media part is removed and not intended to be re-used, the HDO should securely destroy the storage
1099 media part, and where destruction is not feasible, securely remove any patient and organizational data residing on
1100 the storage media prior to disposal.

1101 Where a medical device is decommissioned and disassembled so parts may be reused within the HDO, special care
1102 should be given storage media (e.g. hard drives, USBs, RAM/ROM). Storage media parts should be securely
1103 disposed or have patient and organizational data securely removed from the media prior to reuse. If the storage part
1104 is being inventoried by the HDO for reuse in another similar medical device, or will leave the HDO, the storage part
1105 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:

1153   — Establishes and maintains a medical device security awareness program that communicates security
1154   requirements, industry trends, and other security-related topics to personnel responsible for managing
1155   the security of the organization's medical devices;

1156   — Ensures that security personnel and individuals working on behalf of the organization are informed of
1157   their responsibilities to protect the confidentiality, integrity and availability of medical devices and
1158   sensitive information;

1159   — Directs that security personnel and individuals working on behalf of the organization complete training
1160   within 90 days of hire and at least annually after hire; and

1161   — Ensures that supplemental role-based training be provided to security personnel and individuals
1162   working on behalf of the organization who have a specific business need or whose duties involve
1163   designing, developing, or maintaining the organization's medical devices.

1164   **A.3**   **Supporting security controls and implementation (by organizational function)**

1165   a)   Access Control shall:

1166   — Protect the confidentiality, integrity, and availability of the organization's medical devices by determining
1167   who can access different types of information, and by what means;

1168   — Establish, maintain, document and review/update sufficient controls to restrict physical and logical
1169   access to sensitive information based on a need to know or least privilege basis (i.e., role-based
1170   access); and

1171   — Implement physical, technical, and administrative safeguards to protect all forms of electronic media
1172   (e.g., laptops, CD-ROMs, USB drives, disks, tapes, etc.) containing sensitive information (e.g., patient
1173   data) from unauthorized access.

1174   b)   Human Resources shall:

1175   — Work with the appropriate organization offices (e.g., Human Resources) to establish controls that
1176   ensure security personnel and individuals working on behalf of the organization are suitable for the roles
1177   for which they are placed and are trained on their information security responsibilities;

1178   — Working with IT and other groups within the organization, define, document, and enforce security roles
1179   and responsibilities of security personnel and individuals working on behalf of the organization; and

1180   — Establish, document, and review/update and enforce a formal disciplinary process for colleagues and
1181   individuals working on behalf of the organization who have violated information security policies and
1182   procedures.

1183   c)   Contracting and Outsourcing shall:

1184   — Protect organization medical devices and information that is generated, accessed, stored, transmitted,
1185   processed or otherwise handled by external third parties.

1186   — Establish and maintain a formal process for engaging and assessing the security practices (i.e., vendor
1187   risk) and security design and implementation (i.e., device risk) that is associated with third parties who
1188   provide services and or medical devices that the organization procures.

1189   — Require contraction obligations for reporting and mitigating security vulnerabilities in products (e.g.,
1190   software) or services.

1191   — Terminate business with external third parties who collect, access, store, transmit, process or otherwise
1192   handle organization medical devices and information unless:

1193   • The third-party security requirements are reviewed and approved by security staff.

1194   • A contract is in place stating that the third party has implemented all appropriate administrative,
1195   physical, and technical safeguards.

1196   d)   Compliance shall:

1197   — Ensure that the design, operation, use and management of medical devices adheres to applicable laws,
1198   statutory, regulatory or contractual obligations, and information security requirements;

1199   — Establish and maintain a policy, standards, procedures, and guidance to ensure compliance with
1200   applicable laws, statutory, regulatory or contractual obligations, industry leading practices, and audit
1201   procedures; and

1202   —   Establish processes to address failure to comply with the Medical Device Security Policy and
1203   subsequent standards can result in disciplinary actions up to and including termination of employment
1204   for colleagues or terminations of contracts for contractors, partners, consultants, and other entities.

1205   —   Ensure that technical security requirements, appropriate to the nature of the device level of hazard and
1206   security risk, are established.

1207   e)   Asset and Information Management shall:

1208   —   Establish and maintain an asset management program to track medical device assets, assign
1209   ownership and responsibilities and associate medical device assets with threat and vulnerability
1210   information;

1211   —   Establish and maintain formal media sanitation policy for secure erasure of sensitive information; and

1212   —   Ensure that technical security requirements are enforced.

1213   f)   Business Continuity shall:

1214   —   Ensure that strategies and plans are in place to counteract interruptions to device operations and to
1215   protect critical device operational processes from the effects of major failures of system components or
1216   disasters and to ensure their timely resumption; and

1217   —   Establish and maintain a business continuity program to quickly resume device operational activities
1218   and recover information in the event of system failure or other disaster.

1219   g)   Systems Engineering shall:

1220   —   Establish and maintain a secure lifecycle design program that incorporates security into the device at
1221   the initial design and requirements stage; and

1222   —   Conduct risk assessments for legacy and discontinued devices, and implement extra security controls
1223   (e.g., segmentation) for devices that have reached end-of-life and are no longer supported.

1224

1225

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.

1273   d)   When offering services via HTTP, include identifying strings in HTTP headers. Similarly, when offering other
1274   text-based services, include version numbers and make/model identifiers in header fields or text banners
1275   (greetings).

1276   e)   Respond to SNMP queries on the standard SNMP port (161). Especially, publish the system.sysName.0 and
1277   system.sysDescr.0 variables under the "public" community string.

1278   f)   Consider periodically sending beacons to announce the device's identity. Such protocol options include the
1279   Link Layer Discovery Protocol (LLDP), Cisco Discovery Protocol (CDP) and Simple Service Discovery
1280   Protocol (SSDP).

1281   g)   Support TCP port scanning (e.g. Nmap) (both TCP SYN scanning and TCP connect scanning). Be aware
1282   that port scanning has been known to crash medical devices; the device should be thoroughly robust against
1283   this type of scanning. Test thoroughly with port scanners in the lab before release.

1284   h)   Support a Universally Unique Identifier (UUID); The device identifies itself using a UUID at startup, and/or on
1285   demand. IEEE 11073 SDC profile (OpenSDC) is based on Device Profile for Web Services (DPWS) which
1286   requires a UUID.

1287   i)   Ensure that every product line has an unambiguous name, and that each release of the product has a
1288   version identifier. Version identification is essential to management of patches and updates. If the version of
1289   the software cannot be reliably identified, and whether a patch has been applied or not, the patch process is
1290   not in control, and vulnerabilities cannot be reliably mitigated.

1291   j)   Design network protocols such that endpoints exchange version information. This would include the
1292   category of applications that authenticate using e.g. SSL/TLS.

1293   k)   Publish details about how to identify the version of a device by its network traffic.

1294 Generic hardware platforms hosting health software applications should also identify themselves. In this case the
1295 hardware platform and application should both be identifiable. For example, the hardware platform could use the
1296 DHCP or NAC techniques, while the application identifies using HTTP strings or TLS. Ideally, there is a mechanism to
1297 correlate the application identifier to the host hardware identifier so they can be seen as a pair.

1298 Alternatively, if the IT network assumes responsibility for hardware registration and verification, only the application
1299 may need to identify itself as a medical device.

1300 In the following table maps these techniques according to their effort, their applicability to the operating environment,
1301 and the level of security assurance provided by the technique.

1302   **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) medium otherwise
4	HTTP headers	low (if web server supported)	a, b, c, d, e, f, g, i	challenge resp./hash: medium plaintext: low
5	SNMP	low (if SNMP already supported)	a, b, c, d, e, f, g	high if authenticated 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 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 low otherwise
12	Network traffic profile	medium	a, b, c, d, i	medium

1303

B.1.3 Asset identification

1305 Whether the device security is managed as part of a HDO network, by the manufacturer, or as standalone device, the
1306 assets that are to be protected need to be identified. The manufacturer should provide a list of the assets contained in
1307 the medical device which are potentially in scope for and HDO that is monitoring the effectiveness of the security
1308 measures. This list of assets will help to determine the Security Information and Event Management (SIEM)
1309 monitoring that needs to be performed and the Events of Interest (EOI) that need to be detected and evaluated.

B.1.4 Authorization servers

1311 HDOs commonly use centralized authorization services such as Active Directory Domain Services. Tools such as
1312 these allow a device to offload the administration of authorization and role management and to allow use of standard
1313 IT tools for monitoring and logging authorization events.

B.1.5 Structure of healthcare delivery organization networks

1315 HDOs typically divide their host populations into at least three separate networks: clinical networks, general-purpose
1316 networks, and guest networks. Clinical networks typically include only those hosts on which clinical operations
1317 depend and these hosts are typically given highest priority in cases of congestion. Lowest priority goes to guest
1318 networks, which are typically given access to the Internet but not to any other internal networks. Desktop workstations
1319 and servers often appear on catch-all general-purpose networks. Any of these networks can be subdivided.

1320 Clinical networks are often subdivided by modality, with functions such as surgical care and imaging using different
1321 (often segregated) networks. Security teams generally filter incoming and outgoing traffic flows to, from, and between
1322 these subnetworks to block all traffic not required for essential functions. Designers should expect devices to be
1323 placed on a subnetwork and should not depend on external services being reachable from devices. Designers should
1324 document their devices' typical network behavior so that HDOs can make appropriate changes to network
1325 configuration (e.g., firewall filtering rules).

B.1.5.1 Small clinic networks

1327 Small clinics typically do not have the resources that a large HDO's IT department can deploy. It is unlikely that such
1328 an organization will have a mature security risk management process, sophisticated network analysis tools, or
1329 intrusion detection systems. They will often rely on the manufacturer to manage the security of the device and to
1330 provide details of vulnerabilities and of updates that need to be applied.

B.1.5.2 Home healthcare environments

1332 End users in a home healthcare environment tend to be very trusting and willing to carry out steps communicated to
1333 them by an official sounding voice or email. It is unreasonable to expect these users to perform any configuration or
1334 maintenance tasks related to security. The device may not be remotely accessible, or it may be accessible through
1335 the end users Wi-Fi connection with rudimentary or no security in place. Monitoring and maintenance, if performed at
1336 all, are typically performed remotely.

B.2 Security monitors and logging

1338 NIST SP 800-64 indicates that "The ultimate objective of continuous monitoring is to determine if the security controls
1339 in the information system continue to be effective over time in light of the inevitable changes that occur in the system

1340 as well as the environment in which the system operates". HDOs should not only monitor for undesirable events but
1341 also monitor the effectiveness of risk control measures. For example, monitoring the state of the firewall, responses
1342 to denial of service (DoS) attacks, and authentication events as a consequence of policies set.

1343 A SANS Institute article "Successful SIEM and Log Management Strategies for Audit and Compliance" instructs "a
1344 single common denominator for all regulations requires that one log all events, and review them". In order to log
1345 events, the device needs to be monitoring assets and activities.

1346 Design features that enable security monitoring and logging are essential to enabling security risk management on
1347 deployed devices. There are also industry compliance expectations that require an audit trail.

1348 Service-oriented Architectures (SOA) present a slightly different challenge as many of the traditional tools (scanners,
1349 intrusion detection systems, etc.) are not as suitable for evaluating the security posture of a service-oriented
1350 architecture. NIST SP 800-94 "Guide to Intrusion Detection and Prevention Systems" provides detailed information on
1351 types of and uses for Intrusion detection systems. However, post-processing of security logs can be considered
1352 intrusion detection. More sophisticated users routinely apply machine intelligence to identify intrusions and exploits.

1353 Data gathered as part of a monitoring effort can be used either real-time to generate security status information or as
1354 part of a periodic analysis or audit. Either way, essential feedback is given on the risk management in place. The
1355 nature of the data collected and the processing thereof will be influenced by privacy regulations. Care should be
1356 taken to anonymize all collected data.

1357 **B.2.1 Passive monitoring**

1358 Passive device fingerprinting relies on identifiable device behaviors and often on correct use of network numbers.
1359 Device designers should assign devices MAC addresses from company-owned MAC range allocations, and they
1360 should include appropriate identifying strings when using network services such as mDNS or DHCP.

1361 Once the assets of a device that require protection from security threats are identified, steps can be taken to monitor
1362 some of these assets, including:

1363 — the performance of a device can be compromised by denial of service attacks or malware using device
1364 resources;

1365 NOTE   Flow analysis, or "netflow," relies on special router features that announce network connections to a centralized
1366 collection point. HDOs often look for characteristic flows when trying to identify networked assets. Device designers
1367 should provide HDOs with documentation of the ports and external services the device expects to use.

1368 — devices that can autonomously monitor CPU and memory usage and traffic patterns on interfaces;

1369 — the creation, storage, transmission, or removal of PII on the device;

1370 — administrative records, such as user profiles, authentication services, service records;

1371 — review of monitoring logs.

1372 Other tools used can include anti-virus applications.

1373 Policy violations should be monitored. Actions to take when a policy is violated will depend on the policy, the severity
1374 of the violation, the intended use of the device, and the current state of the device; e.g. lockdown of the device may
1375 not be feasible if it is engaged in life-sustaining activities. All authentication events and data transfers should be
1376 monitored.

1377 Periodic archiving and removal of PII is recommended. The device should monitor for the presence of PII, facilitate
1378 the cleanup activity, and monitor (i.e., log) the occurrence or absence of cleanup events, whether manual or
1379 automated.

1380 The scope of the assets and data to be monitored should be chosen carefully, weighing the overhead and
1381 management of data against the usefulness of that data for predictive or post-event processing. Often it is not a
1382 single monitoring information source but rather the correlation of monitored data that indicates a security issue, and
1383 that facilitates locating the intrusion and the impacted assets. Further design considerations can include malware
1384 monitoring (including anti-virus engines) and intrusion detection. Intrusion detection tools are generally deployed at a
1385 network level rather than on the device itself.

1386 It remains a design decision whether to include the correlation and interpretation of the data as an activity on the
1387 device to facilitate notifications, or whether to do it remotely using a SIEM system.

1388 The scope of the monitoring performed and the analysis of the accumulated data will be heavily influenced by the
1389 deployment model, since logging large amounts of data on a device that is rarely connected will not be feasible. An
1390 architecture that supports prioritization of logged events, log rotation, and configurable logs is advisable when a
1391 device is to be deployed in varied environments.

1392 The design should ensure that sufficient storage and bandwidth resources are available for the maintenance and
1393 transmission of the data that is generated from monitoring activities.

1394 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

1396 Essential to detecting threat events is a forensic, tamper-resistant security log. A potential way to achieve this is to
1397 implement an append-only log with authenticated chain of custody. Logging options include:

1398 — a dedicated logging sink on the local network with device and system logs streaming to it in real time or
1399   "often" (e.g. every few minutes);

1400   NOTE   This should include a built-in alert when logger cannot cope with load or is almost out of storage.

1401 — an off-site logger with requirements similar to the local logging sink above, with a caching or contingency
1402   plan if external connection is unavailable;

1403 — confidential (encrypted at-rest), tamper-evident and tamper-resistant hardware;

1404 — meta-log for access to the logger and/or attempts to delete or alter information;

1405 — authentication and authorization system for logger;

1406 — a change tracking system with attribution and ability to revert.

1407 Device manufacturers should consider a log interface exposed for log collection as distinct from collecting the logs
1408 (NIST SP 800-92). A "standardized" interface for frequent log export combined with a "black box"-type attachment for
1409 devices is recommended.

1410 Log entries should have timestamps relative to the device rather than the network as the timing and sequence of
1411 events has meaning. Other techniques to consider with logging include:

1412 — authoritative logger real-time clock;

1413 — best practices: e.g. Vector clocks or other strong sequence-preserving techniques;

1414 — independent timestamping of all messages by sender, preferably using an authoritative logger clock. If the
1415   sender has no real-time clock capabilities, a sequence number can be used.

1416 Origin authentication, encryption, and validation of the log is recommended. If chain of custody is too onerous for a
1417 single device, it should still be considered for the network. In support of the authenticity of logs, the following may also
1418 be considered:

1419 — tamper-evident and tamper-resistant hardware, including append-only logs;

1420 — confidential (encrypted at-rest), authenticated (e.g., signed messages and Merkle trees for signature
1421   aggregation and bulk verification) storage;

1422 — off-site backup using separate encryption and authentication keys, performed in near-real-time;

1423 — meta-log for access to the logger and/or attempts to delete or alter information;

1424 — authentication and authorization system for logger;

1425 — change tracking system with attribution and ability to revert.

B.1.1   Active monitoring

1427 Active monitoring entails injecting test data or instructions to the device to ascertain the effectiveness of security
1428 controls. Consider it a controlled experiment where observed results can be compared to expected results. A
1429 common version of this is an application that simulates user activity. The user can be an expected user with a defined
1430 role (e.g., to determine that if role-based security measures are operating as expected) or an adversarial user (e.g.,

1431 attempting a brute force password hacking attack or a DoS attack. Other tools used include port scanning,
1432 vulnerability scanning, and penetration testing.

1433 HDOs, like any enterprise, routinely use port scanning to check for changes in the set of services that networked
1434 hosts are running. Manufacturers should port-scan their own devices under realistic network conditions to ensure that
1435 doing so does not trigger bugs or cause crashes. Popular open-source port scanners can be tuned for
1436 aggressiveness; designers should make sure to test the most aggressive settings.

1437 Vulnerability scanners are also in common use. These software tools run a barrage of tests for known vulnerabilities.
1438 Device designers should already be using security scanners to test their own products during design phases, but
1439 frequent scanning during all phases of product development should minimize the chance of postmarket problems
1440 attributable to scanning.

1441 These tools tend to be part of the IT network infrastructure and not usually included as a feature on the device.

1442 **B.1.2   Security logs**

1443 NIST SP 800-92 "Guide to Security Log Management" provides a rich background on security logging including the
1444 types of logs, the challenges, and design and infrastructure issues associated with logging.

1445 The SANS Consensus Policy Resource Community: Information Logging Standard document is a useful checklist for
1446 a designer attempting to decide what needs to be logged.

1447 The data generated from these monitoring activities, often described as security logs, should be protected from
1448 tampering while at rest and during transmission. Other considerations include:

1449   a) handling uncertainty in the log data;

1450   — known unknowns;

1451   When analyzing logged activity, do not ignore events of uncertain or unclear meaning. If there are log
1452   entries or events in the logs that cannot be identified or for which there is no coinciding incident (e.g. an
1453   exploit) or medical event, there may still be an issue, e.g., early indications of installation of malware
1454   that is not activated until months later. Retrieve and analyze the logs regularly to assure the correct
1455   operation of logging and the effectiveness of the filtering.

1456   — unknown unknowns.

1457   Periodically reevaluate what is being logged and what can be determined about your device or network
1458   from those logs. Regularly re-evaluate your rules or filters for the logs; Ensure that the data extracted
1459   from the logs matches explicit requirements for auditing or identification. Evaluate whether new rules or
1460   patterns need to be added based on known vulnerabilities or exploits.

1461   b) device-only versus system interaction data;

1462   Logs of systems or networks as well as individual device logs are a useful source of information for security
1463   monitoring, Post-processing of device and system logs can be cross-correlated to generate information on
1464   interactions and events that are not obvious at the device level. E.g. man-in-the middle attacks might be
1465   detected in this fashion. Institutions increasingly use machine-learning based tools to obviate the need for
1466   laborious manual correlation of all possible interactions.

1467   c) security data retrieval and use environment.

1468   While access to the logs or analytics may be well defined for large HDOs, smaller organizations may have
1469   fewer tools in place and fewer rules around access to logged data. Remote devices in a home healthcare
1470   environment or satellite clinics will still need to be monitored. It is important that the service agreement for
1471   the device includes provision for the security monitoring model. Post-processing may be the only option for
1472   remote devices.

1473 The design should consider the means of access to the data. The solution will differ based on the network
1474 connectivity of the device, the model for processing the data, and the storage capabilities of the device. The device
1475 security logs may be kept on the device, sent periodically to a collection point (log server), or streamed to a log
1476 analyzer for real-time analysis.

1477 Failsafes should exist for events that prevent the device from transmitting the logs upstream. For example, different
1478 categories of threat events can be defined, and retention of higher priority event logs prioritized over logs of lower
1479 category events.

1480 Access to this data should be restricted to the appropriate roles. To facilitate this, and to comply with privacy rules, it
1481 is advisable that security logs remain independent of system and clinical logs, although there may be some events
1482 that fall into multiple logging categories. Logging features need to identify what logged data is for use by the end-
1483 user, and what is for use by Manufacturers. It is expected that the majority of security logs would be for the end-user,
1484 and manufacturer's logs would be limited to service or system logs. A feature that relies on the device "phoning
1485 home" in order to deliver logs to a manufacturer may not satisfy privacy or HDO IT-network rules and should not be
1486 relied upon.

1487 Guides to security log management exist, albeit not specific to medical devices, for example:

1488   a) NIST SP 800-92 Guide to Computer Security Log Management;

1489   b) SANS Consensus Policy Resource Community: Information Logging Standard, 2014;

1490   c) UL2800-0 DATA LOGGER and DATA STORE Requirements.

1491 **B.2   Design pitfalls**

1492 Intrusion detection tools, and the countermeasures deployed, can have a detrimental effect on the intended use of
1493 the device. Tools and countermeasures should be carefully vetted for side-effects.

1494 Prioritizing logging and monitoring to the detriment of intended use is also to be avoided. Logging and monitoring
1495 schemes should be designed such that they do not affect the intended use of the device, and are generally also not
1496 visible to the user of the device.

1497 In the pursuit of greater security, manufacturers and integrators may be tempted to add multi-factor, role-based
1498 authorizations schemes. Authorization restrictions should not impair availability during intended use. The device
1499 architecture should support varying levels of role-based access where on-demand services are immediately
1500 accessible and others such as log retrieval are only accessible with the correct authorization.

Annex C
1501
1502 (Informative)
1503
1504 **Establishing a coordinated vulnerability disclosure process**

1505 **C.1   Accepting vulnerability information from external sources**

1506 Medical device manufacturers should develop a robust vulnerability handling and coordinated disclosure processes to
1507 ensure that their products' residual risk is maintained at an acceptable level throughout the postmarket phase.
1508 Various procedural communicative and technical aspects of a well-designed process will assist in meeting this goal.

1509 ISO/IEC 29147:2014 *Information Technology – Security Techniques – Vulnerability Disclosure* and ISO/IEC
1510 30111:2013 *Information Technology – Security Techniques – Vulnerability Handling Processes* should be used by
1511 manufacturers as the basis for establishing their own vulnerability handling and responsible disclosure processes.
1512 Figure C.1 from ISO 29147:2014 provides a visual representation of how the two processes of vulnerability disclosure
1513 and vulnerability handling are tightly coupled:
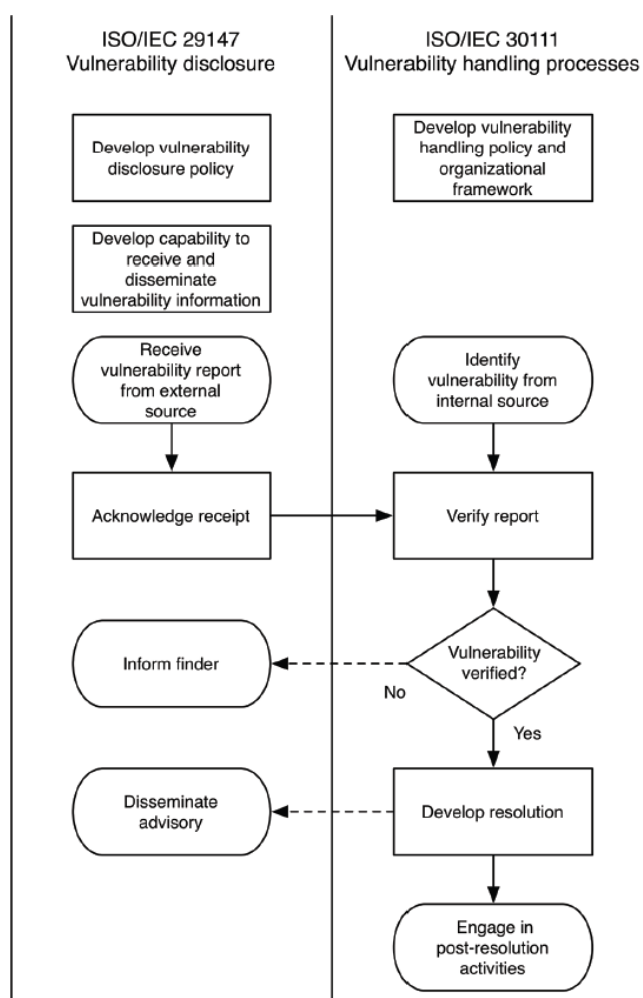
1514

1515
1516   **Figure C.1 — A module of the interface between ISO/IEC 29147 and ISO/IEC 30111**

1517   There are two key aspects of a successful vulnerability and responsible disclosure policy:

1518   — established internal process for accepting vulnerability information received from external sources;

1519   — established external and internal process for effectively communicating to the manufacturer's customers and
1520   users' important information regarding the recently disclosed known common vulnerability and exposures
1521   (KCVEs) pertaining to the manufacturer's medical device products.

1522   **C.2   Accepting vulnerability information from external sources**

1523   In situations where an external source (e.g. security researcher) is attempting to establish contact with an appropriate
1524   information security representative from a manufacturer, it is important for the manufacturer's policy and external
1525   presence (e.g. web site) to be clear and explicit. The appropriate communication channel should be indicated, such
1526   as a dedicated group e-mail and telephone number as the most expeditious manner for the external source to contact
1527   the manufacturer and report the KCVE. Relying on generic customer support telephone numbers or email addresses
1528   is not optimal and may result in a possible excessive delay in responding. A KCVE notification directed to an
1529   employee not versed in security, or the request and source being transferred between multiple employees, or the
1530   request being lost before reaching the correct information security engineering representative could be catastrophic.
1531   In all of these examples, the external source reporting the KCVE could lose confidence in the manufacturer's process
1532   and possibly defer, out of frustration, to other another method such as a preemptive public disclosure. In these
1533   examples the manufacturer loses credibility and forgoes the opportunity to proactively confirm, verify and mitigate the
1534   potential cybersecurity and/or safety risk to patients.

1535   Additionally, by having a streamlined responsible disclosure and vulnerability reporting process, this cybersecurity
1536   program maturity allows external reporting sources an opportunity to provide information on potentially unknown
1537   KVCEs and other product security vulnerabilities. The manufacturer should provide clear information to facilitate
1538   establishing a cooperative relationship with the KCVE reporting source always with the end goal of finding solutions
1539   that reduce the risks associated with a vulnerability.

1540   Proactive and actionable activities should include

1541   — direct communications channel to contact the manufacturer (with a secure option provided, such as PGP
1542   enabled e-mail);

1543   — responsible disclosure and vulnerability reporting scope statement providing guidance of the goal of the
1544   disclosure process;

1545   — details on the medical device information to be provided (e.g., product model, product serial number,
1546   configuration details, scenario to reproduce vulnerability);

1547   — request for contact information for the reporting source – including phone numbers, e-mail address and PGP
1548   key;

1549   — expected initial response time to the reporting source;

1550   — specific steps the manufacturer is expected to perform with the information provided (e.g., attempt to
1551   reproduce);

1552   — manufacturer's expectations on reporting source's actions (e.g. never perform test on medical devices in
1553   active or clinical use scenarios such as a hospital networked environment).

1554   **C.3   Process for communicating to users and reporting known vulnerabilities**

1555   When a vulnerability is reported by an external source, the manufacturer should ensure the source is kept informed
1556   as appropriate on planned remediation efforts.

1557   Once a remediation (e.g. compensating control, product update, software patch) is established, and successfully
1558   applied by the customer of the manufacturer, the final responsibility of a manufacturer's vulnerability disclosure
1559   process is to ensure that KCVE remediation information is disseminated as widely as possible. Depending on the
1560   vulnerability and the architected remediation, this process is divided into two main categories of actions; (1)
1561   customers, and (2) other governmental agencies (OGA). With regard to category (1), the list of parties to disclose to
1562   should include direct communication with patients, informing physicians, technical details being passed to HDO IT
1563   departments.

1564   Within category (2), the KCVE details are written in the form of a KCVE narrative. The narrative is then reviewed with
1565   the US-Computer Emergency Response Team (US-CERT). US-CERT as part of the Department of Homeland
1566   Security (DHS) then will re-assign the proposed KCVE narrative to the Industrial Control System (ICS)-CERT. Once
1567   the approving authority, in the most general of cases, the ICS-CERT, located within the Idaho National Laboratory,

1568 approves the agreed upon KCVE with the manufacturer, then the KCVE is released to the SECURE US-CERT Portal
1569 for secure access up to 30 days. After 30 days the US-CERT will release to the general public with a courtesy
1570 notification to the FDA.

1571 Additional sources who could potentially report cybersecurity vulnerabilities to a manufacturer:

1572 — threat information vendors;

1573 — US-CERT;

1574 — CVE-Details.com;

1575 — MITRE CWE;

1576 — MITRE CVE;

1577 — NIST NCCoE;

1578 — DHS;

1579 — OGAs.

1580 **C.4   Importance of third-party applications, firmware, and hardware**

1581 Another important aspect of a manufacturer's full lifecycle cybersecurity support for a product is to ensure that known
1582 common vulnerabilities and exposures that affect third-party software/hardware components are monitored and risk
1583 assessed. Medical devices have numerous third-party components which are all vulnerable to compromise. It is
1584 critically important that the KCVEs of these third-party applications, firmware, and hardware are also accounted for,
1585 tracked, and identified. Whenever possible, KCVEs should be remediated via software patch, firmware upgrade or
1586 appropriate compensating control.

1587 Every manufacturer should have a robust process in place to identify the third-party components used in its products,
1588 track vulnerabilities against those components, access the impact of those vulnerabilities to the medical device,
1589 implement appropriate remediation(s), and communicate appropriate information on these details to customers. If
1590 common third-party components are used (e.g. operating systems), it is expected that many vulnerabilities will be
1591 reported to the larger IT community via platforms such as the National Vulnerability Database.

1592 **C.5   U.S. FDA recognition of consensus standards (country-specific)**

1593 Irrespective of the originating source, a clear, consistent, and reproducible process for intake and handling of
1594 vulnerability information should be established and implemented by the manufacturer. FDA has recognized ISO/IEC
1595 30111:2013 *Information Technology – Security Techniques – Vulnerability Handling Processes* that may be a useful
1596 resource for manufacturers.

1597 Manufacturers should also adopt a coordinated vulnerability disclosure policy. FDA has recognized ISO/IEC
1598 29147:2014 *Information Technology – Security Techniques – Vulnerability Disclosure* that may be a useful resource
1599 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 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: **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.]

Defined terms - Postmarket Management of Cybersecurity in Medical Devices	ANSI/AAMI/ISO 14971:2007	TIR97
B. Controlled Risk 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: **2.15** **residual risk** risk remaining after risk control measures have been taken NOTE 1 Adapted from ISO/IEC Guide 51:1999, definition 3.9. 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"). 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 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"). The definition of residual risk is identical to the one incorporated in ISO 14971:2007 and AAMI TIR57:2016.
D. Cybersecurity Signal 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. 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: **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.]

Defined terms - Postmarket Management of Cybersecurity in Medical Devices	ANSI/AAMI/ISO 14971:2007	TIR97
E. Exploit 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"). The standard defines a "hazardous situation" as: **2.4** **hazardous situation** circumstance in which people, property, or the environment are exposed to one or more hazard(s) [ISO/IEC Guide 51:1999, definition 3.6] 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: **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.]
F. Patient Harm 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": **2.2** **harm** physical injury or damage to the health of people, or damage to property or the environment [ISO/IEC Guide 51:1999, definition 3.3]	The definition of "harm" is identical to the one used in AAMI TIR57:2016: **2.11** **harm** 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 [SOURCE: IEC 80001-1:2010, definition 2.8]
G. Remediation 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. 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"). 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 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: **2.28** **threat** 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 NOTE 1 to entry: Identical to NIST definition (SP 800-53) with the phrase "or the Nation" redacted. [SOURCE: SP 800-53; SP 800-53A; SP 800-27; SP 800-60; SP 800-37; CNSSI-4009]
I. Threat modeling 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 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"). 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 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: **2.34** **vulnerability** weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source [SOURCE: SP 800-53; SP 800-53A; SP 800-37; SP 800-60; SP 800-115; FIPS 200]

1605

1606   **Bibliography**

1607

1608   [1]   ANSI/AAMI/ISO 14971:2007, *Medical devices - Application of risk management to medical devices.*
1609   Association for the Advancement of Medical Instrumentation; 2007. Arlington, VA.

1610   [2]   ANSI/AAMI/ISO TIR24971:2013, *Guidance on the application of ISO 14971.* Association for the Advancement
1611   of Medical Instrumentation; 2013. Arlington, VA.

1612   [3]   ANSI/AAMI/IEC 80001-1:2010, *Application of risk management for IT networks incorporating medical devices -*
1613   *Part 1: Roles, responsibilities and activities.* Association for the Advancement of Medical Instrumentation;
1614   2010. Arlington, VA.

1615   [4]   AAMI/ANSI/IEC, TIR 80001-2-2:2012, *Application of risk management for IT networks incorporating medical*
1616   *devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and*
1617   *controls.* Association for the Advancement of Medical Instrumentation; 2012. Arlington, VA.

1618   [5]   FDA, *Postmarket Management of Cybersecurity in Medical Devices.*
1619   https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022
1620   .pdf (Accessed 06 February 2018)

1621   [6]   HIMMS/NEMA   Manufacturer   Disclosure   Statement   for   Medical   Device   Security   (MDS2).
1622   http://www.himss.org/resourcelibrary/MDS2

1623   [7]   IEC TR 80002-2-8:2016, *Application of risk management for IT-networks incorporating medical devices - Part*
1624   *2-8: Application guidance - Guidance on standards for establishing the security capabilities identified in IEC TR*
1625   *80001-2-2*

1626   [8]   NIST SP 800-61 Rev. 2, *Computer Security Incident Handling Guide*

1627   [9]   NIST SP 800-64 Rev. 2, *Security Considerations in the System Development Life Cycle*

1628   [10]   NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*

1629   [11]   NIST SP 800-92, *Guide to Computer Security Log Management*

1630   [12]   NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Information Systems and Organizations*

1631   [13]   NIST SP 800-88 Rev. 1, *Guidelines for Media Sanitization*

1632   [14]   NIST SP 800-30 Rev. 1, *Guide for Conducting Risk Assessments*

1633   [15]   NIST   NISTIR   7298,   Rev.   2,   *Glossary   of   Key   Information   Security   Terms*,   May   2013.
1634   http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

1635   [16]   *SANS Consensus Policy Resource Community: Information Logging Standard*, 2014

1636   [17]   *Best Practices: Event Log Management for Security And Compliance Initiatives.* Ipswitch Inc. 2010
1637   https://www.ipswitch.com/Ipswitch/media/Ipswitch/Documents/Resources/Whitepapers%20and%20eBooks/EL
1638   M_Security_WP.pdf?ext=.pdf

1639   [18]   "Successful SIEM and Log Management Strategies for Audit and Compliance"; SANS Institute, 2010