



Healthcare & Public Health
Sector Coordinating Councils

PUBLIC PRIVATE PARTNERSHIP

1
2

3 MEDICAL DEVICE AND HEALTH IT
4 JOINT SECURITY PLAN

5 January 2019

6
7
8
9
10

11
12
13
14
15
16
17

18
19 **ABOUT THE HEALTHCARE AND PUBLIC HEALTH**
20 **SECTOR COORDINATING COUNCIL**
21 **JOINT CYBERSECURITY WORKING GROUP**

22
23 The Healthcare and Public Health Sector Coordinating Council (HSCC) is a coalition of private-
24 sector, critical healthcare infrastructure entities organized under Presidential Policy Directive 21
25 and the National Infrastructure Protection Plan to partner with government in the identification
26 and mitigation of strategic threats and vulnerabilities facing the sector’s ability to deliver
27 services and assets to the public. The HSCC Joint Cybersecurity Working Group (JCWG) is a
28 standing working group of the HSCC, composed of more than 200 industry and government
29 organizations working together to develop strategies to address emerging and ongoing
30 cybersecurity challenges to the health sector.

31
32 This Medical Device and Health IT Joint Security Plan is the product of a task group established
33 under the auspices of the HSCC JCWG and composed of medical technology, health IT and
34 health delivery organizations, as well as the FDA, to address a major recommendation of the
35 Health Care Industry Cybersecurity Task Force report from June 2017 calling for a cross-sector
36 strategy to strengthen cybersecurity in medical devices.

37
38 To provide feedback on this tool, please send comments to:
39 **JSPFeedback@HealthSectorCouncil.org**

40
41 For more information on the HSCC, see <https://HealthSectorCouncil.org>.

42	Contents	
43	Acknowledgments	4
44	Executive Summary	7
45	Background	7
46	Purpose and Objectives	8
47	JSP Product Security Framework Overview	9
48	How to Use the JSP	10
49	JSP Product Security Framework Implementation	11
50	Evaluating JSP Progress and Maturity	22
51	Appendix A: Acronyms	28
52	Appendix B: Terminology	29
53	Appendix C: Roles and Responsibilities	33
54	Appendix D: Drafting of the Joint Security Plan	35
55	Appendix E: Example Design Input Requirements for Security	39
56	Appendix F: Example Third-Party Security Agreement	41
57	Appendix G: Example Customer Security Documentation	43
58	Appendix H: Example Organizational Structure	47
59	Appendix I: Example Organizational Training	49
60	Appendix J: Example Security Risk Assessment Methods	51
61	Appendix K: CMMI® for Development	51
62		
63		
64		

65 **I Acknowledgments**

66 The following individuals constitute the membership of the committee established in November
67 2017 who were responsible for development of the Medical Device and Healthcare Information
68 Technology Joint Security Plan.

- 69 • **Task Group Co-Chair**, Kevin McDonald, Director of Clinical Information Security, Mayo
70 Clinic
- 71 • **Task Group Co-Chair**, Rob Suarez, Director of Product Security, Becton, Dickinson &
72 Company
- 73 • **Task Group Co-Chair**, Aftin Ross, Senior Project Manager, Center for Devices and
74 Radiological Health (CDRH) at US Food and Drug Administration
- 75 • Bill Hagestad, Independent Information Security Researcher
- 76 • Colin Morgan, Director, R&D & Product Security, Johnson & Johnson
- 77 • Jim Jacobson, Chief Product and Solution Security Officer, Siemens Healthineers
- 78 • Michael McNeil, Global Product Security & Services Officer, Philips
- 79 • Seth Carmody, Cybersecurity Project Manager, CDRH at US Food and Drug
80 Administration
- 81 • Zach Rothstein, Vice President, Technology and Regulatory Affairs, AdvaMed
- 82 • Ronald Mehring, Chief Information and Security Officer/VP of Technology, Texas Health
83 Resources
- 84 • Hitesh Patadia, Enterprise Architect, Alberta Health Services
- 85 • Christopher Bennett, Senior Information Security Analyst, Medical University of South
86 Carolina
- 87 • Greg Garcia, Executive Director at Healthcare Sector Coordinating Council
- 88 • Suzanne Schwartz, Associate Director for Science and Strategic Partnerships, CDRH at US
89 Food and Drug Administration
- 90 • Caleb Eggink, Security Solution Leader, Cerner
- 91 • Ali Nakoulima, Lead Technology Architect, Cerner
- 92 • Regina Geierhofer, Regulatory Affairs Manager, Cerner
- 93 • John Travis, Vice President Regulatory Research, Cerner

- 94 • Ray Smith, Lead Software Engineer, Cerner
- 95 • Greg Thole, Senior Regulatory Strategist, Cerner
- 96 • Wil Vargas, Standards Director, Association for the Advancement of Medical
97 Instrumentation
- 98 • Jim Hanson, Information Security Officer, Avera Health
- 99 • Ashley Woyak, Business Information Security Officer, Baxter Healthcare Corporation
- 100 • Ken Hoyme, Director of Product Security, Boston Scientific
- 101 • Michael Maksymow, CIO, Beebe Healthcare
- 102 • Michael Seeberger, Systems Engineer, Boston Scientific
- 103 • Mari Rose Savickis, Vice President of Federal Affairs, CHIME
- 104 • Fernando Blanco, CHRISTUS Health, VP & CISO
- 105 • Aaron Wishon, CISO, Cook Children’s Health Care System
- 106 • Clyde Hewitt, Vice President, Security Strategy / NCHICA Board of Directors,
107 CynergisTek/NCHICA
- 108 • David Klonoff, President, Diabetes Technology Society
- 109 • Charles Stride, Senior VP, CIO/CISO, Holy Redeemer Health System,
- 110 • Paul Connelly, VP/CISO, HCA Healthcare
- 111 • Peter Amadio, Professor of Biomedical Engineering, Mayo Clinic (AEHIS)
- 112 • Greg Garneau, CISO, Marshfield Clinic Health System
- 113 • Lisa Griffin Vincent, VP of Clinical Science, Medical Device Innovation Consortium
- 114 • Elliott Warren, Director of Federal Affairs, Medical Device Manufacturers Association
- 115 • Zack Hornberger, Director of Cybersecurity & Informatics, Medical Imaging Technology
116 Association
- 117 • Matt Russo, Sr. Director of Global Security Office, Medtronic
- 118 • Ari Entin, CIO, Natividad Medical Center (AEHIS)
- 119 • Katie Boyer, Manager of Policy and Advocacy, Nemours Children’s Health System

- 120 • Jon Crosson, Manager of Special Interest Group Services, H-ISAC
- 121 • Nathan Gibson, CIO, Quality Insights (AEHIS)
- 122 • Dr. Sheila Whalen, DNP, RN-BC, Clinical Integration Program Manager, Rush University
123 Medical Center
- 124 • Kevin Scott, Senior Corporate Director of Security and End User Services, Shriners
125 Hospitals for Children
- 126 • Ross Carevic, Director of Business Technology, Vizient
- 127 • Christine Sublett, President &Principal Consultant, Sublett Consulting, LLC
- 128 • Alex Reniers, Cyber Analyst, US Department of Homeland Security

129

130 The HSCC Joint Cybersecurity Working Group TG-1B drafting committee would also like to
131 thank all of the individuals and organizations within the Healthcare Sector Coordinating Council
132 (HSCC) that reviewed and contributed to the plan.

133

134

135 **II Executive Summary**

136 Software-based medical technologies have the potential to positively impact patient care.
137 However, as these products become more connected, product cybersecurity becomes
138 increasingly important as there is the potential for patient harm and disruption of care if products
139 or clinical operations become impacted because of a cybersecurity concern. As product
140 cybersecurity is a shared responsibility, a wide range of healthcare stakeholders under the
141 umbrella of the Healthcare and Public Health Sector Coordinating Council (HSCC), have drafted
142 this Joint Security Plan (JSP) to address cybersecurity challenges. These challenges include but
143 are not limited to transparency and disclosure between vendors and end users, security by design
144 and throughout the product lifecycle, and product end of life. Specifically, the JSP is a total
145 product lifecycle reference guide to developing, deploying and supporting cyber secure
146 technology solutions in the healthcare environment. It includes:

- 147 • Cybersecurity practices in design and development of medical technology products
- 148 • Handling product complaints relating to cybersecurity incidents and vulnerabilities
- 149 • Managing security risk throughout the lifecycle of medical technology
- 150 • Assessing the maturity of a product cybersecurity program

151 The JSP is voluntary and seeks to aid organizations (medical device manufacturers, healthcare
152 information technology (IT) vendors, and healthcare providers) in enhancing their product
153 cybersecurity irrespective of organization size or maturity. It is intended to be globally
154 applicable, inspire organizations to raise the bar for product cybersecurity, and is expected to
155 evolve as product cybersecurity evolves. As such, it is anticipated that there will be future
156 iterations of the JSP and feedback on this initial version is welcome.

157 It is important for medical device manufacturers (MDMs) and health IT vendors, collectively
158 referred to as vendors, to consider the JSP's voluntary framework and its associated plans and
159 templates throughout the lifecycle of medical devices and health IT because doing so is expected
160 to result in better security and thus better products for patients. Security can be difficult to
161 integrate into existing processes for a variety of reasons such as organizations not recognizing its
162 importance, not knowing where to start, and insufficient resources. The components in the JSP
163 framework are used to help create security policy and procedures that align and integrate into
164 existing processes. Our primary ask of organizations is to make a commitment to implementing
165 the JSP as it is expected that patient safety will be positively impacted as a result.

166

167 **III Background**

168 In the *Cybersecurity Act of 2015* (the Act), the United States Congress established the Health
169 Care Industry Cybersecurity (HCIC) Task Force to identify the challenges that the healthcare
170 industry faces when securing and protecting itself against cybersecurity threats. Industry
171 participation in the task force brought to light critical gap areas warranting focus; year-long
172 discussion and analysis culminated in the release of a set of recommendations and action items to
173 address six high-level imperatives.

174 In 2017, a group of medical device manufacturers stepped up to address the recommendations
175 and action items set forth under Imperative 2 of the HCIC Task Force Report: “Increase the
176 security and resilience of medical devices and health IT” by engaging healthcare delivery
177 organizations in a collaborative effort that would produce a Joint Security Plan. This effort was
178 further formalized under the auspices of the Healthcare Sector Coordinating Council’s Joint
179 Cybersecurity Working Group public-private partnership, as the JSP was broadly socialized with
180 healthcare providers, trade associations, security professionals, and government organizations
181 during development and prior to its release. The U.S. Food and Drug Administration, in its role
182 as a key public sector partner, also assisted with the development of the JSP. For additional
183 information on how the JSP was drafted, please see Appendix D. Imperative 2 of the HCIC Task
184 Force Report states:

185 ***Imperative 2. Increase the security and resilience of medical devices and health IT.***

186 *The Health Care and Public Health (HPH) Sector is charged with keeping patients safe*
187 *and that includes protecting patients from physical harm, as well as privacy-related*
188 *harms that may stem from an exploited known cybersecurity vulnerability. If exploited, a*
189 *vulnerability may result in medical device malfunction, disruption of health care services*
190 *(including treatment interventions), inappropriate access to patient information, or*
191 *compromised EHR data integrity. Such outcomes could have a profound impact on*
192 *patient care and safety. Some foundational challenges that will need to be addressed in*
193 *order to enhance the cybersecurity of medical devices and EHRs include legacy*
194 *operating systems, secure development lifecycle, strong authentication, strategic and*
195 *architectural approaches to product deployment, management, and maintenance on*
196 *hospital networks.*

197 *The relatively short lifespan for operating systems and other relevant platforms such as*
198 *commercial off the shelf software is inherently misaligned in health care as medical*
199 *devices and EHRs may be utilized for 10, 15, 20, or more years. This misalignment may*
200 *occur for a variety of reasons. Hospitals operate on thin budgets and cannot replace*
201 *capital equipment like MRIs as quickly as new operating systems are released. Product*
202 *vendors have a product development lifecycle that may take several years and they may*
203 *start development using one operating system and by the time the product comes to*
204 *market, newer operating systems may be available. Creative ways of addressing the*
205 *aforementioned challenge areas may be found by engaging key clinical and cybersecurity*
206 *stakeholders, including software vendors.*

207
208 The JSP is expected to evolve over time and the HSCC intends to establish a governance model
209 to ensure the baseline strategy is updated based on execution of existing plans or new needs
210 identified by members of the stakeholder community.
211

212 **IV Purpose and Objectives**

213 The HSCC believes that, because medical technology is integral to patient safety and clinical
214 operations, product cybersecurity in medical technology is a shared responsibility among
215 healthcare stakeholders. Moreover, more secure products result in higher quality products
216 which positively impact public health. The JSP is a consensus-based total product lifecycle
217 reference guide for developing, deploying, and supporting cyber secure technology solutions in

218 the health care environment. It is not a regulatory document nor is it a standard. Rather the JSP
219 may be leveraged across an organization’s product portfolio and is intended to be globally
220 applicable. Furthermore, the recommendations provided in the JSP are intended to help
221 organizations of various size and stages of maturity to enhance their product cybersecurity
222 posture by addressing key cybersecurity challenges.

223 This voluntary plan is intentionally forward leaning and seeks to inspire organizations to raise
224 the bar for product cybersecurity. In particular, integrating cybersecurity into an organization
225 necessitates organizational and process changes that come with considerable time and monetary
226 investments. The JSP provides a framework for making these organizational and process related
227 changes.

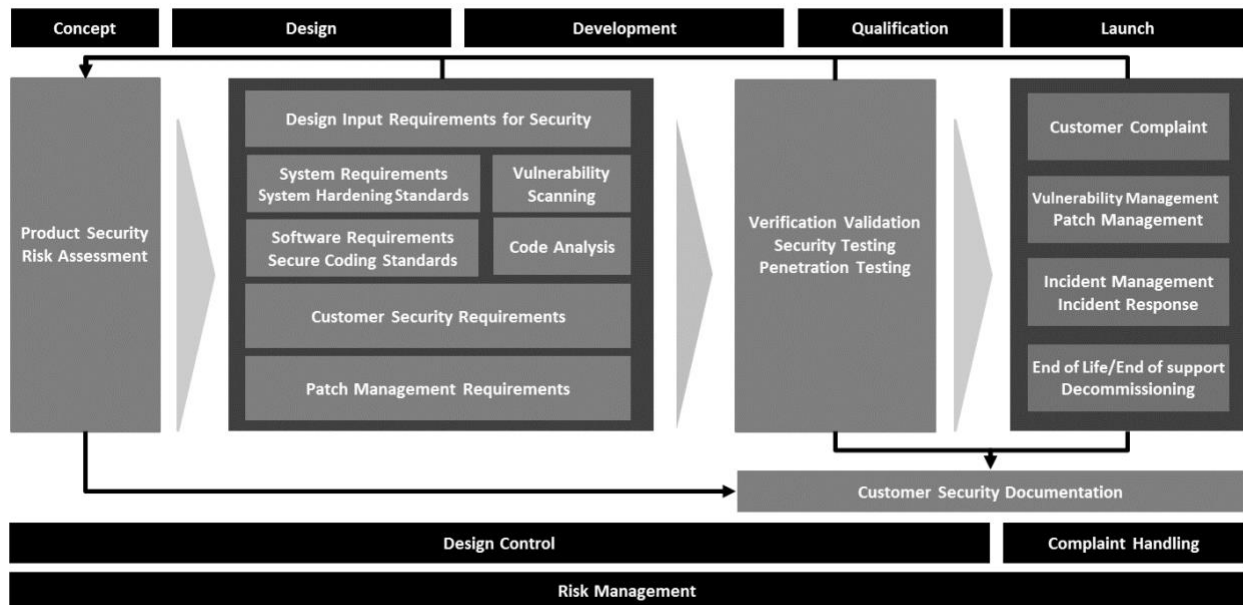
228 One of the main themes of the JSP is the idea of continuous improvement. We encourage
229 medical device manufacturers, health IT vendors, and healthcare providers to make a
230 commitment to adopting the JSP to aid in developing, deploying, and supporting cyber secure
231 technology solutions in the health care environment. The adoption of the JSP, with the
232 integration into current practices, is expected to provide a safer and more resilient patient care
233 and result in overall improved product quality.
234

235 **V JSP Product Security Framework Overview**

236 The JSP framework establishes that effective cybersecurity is integrated into an organization’s
237 quality system processes and is incorporated throughout the various stages of the
238 commercialization process (from concept to launch). Figure 1 provides a framework for
239 incorporating the JSP into existing quality system processes and throughout commercialization.
240 The core of this framework aligns to traditional quality system concepts. Design controls, risk
241 management, design requirements, testing and post market management can be aligned with
242 multiple software development methodologies (not shown). Documentation of the product
243 security activities/processes in the JSP framework core is encouraged to demonstrate that the
244 framework has been applied consistently and is rigorously followed. Healthcare providers
245 seeking further guidance on the secure operation of medical devices, and other information
246 technology used to run their healthcare operations, may refer to HSCC “[Health Industry
247 Cybersecurity Practices \(HICP\): Managing Threats and Protecting Patients](#)” publication, which
248 stems from the Cybersecurity Information Sharing Act of 2014 (CISA) 405(d) effort. Additional
249 guidance and detail are provided for each product security activity or process identified in the
250 JSP framework in Section VII of this document. Acronyms and term definitions used throughout
251 the JSP may also be found in Appendix A and Appendix B respectively.

252

253



254
 255 **Figure 1. Product Security Framework.** Top row represents product commercialization
 256 phases. Core represents product security activities and processes. Two bottom rows represent
 257 quality system processes

258
 259 **VI How to Use the JSP**

260 For the successful use of the JSP, an initial step is to be able to define the governance process as
 261 it relates to organizational roles and responsibilities, and the needs for personnel training.

262 Governance which may include strategic decisions, establishing milestones, and tracking of
 263 maturity against the framework is executed by designated leaders in a vendor’s organization.
 264 Framework adoption should be driven by mapping each of the framework cybersecurity
 265 activities and processes into existing processes and minimizing the creation of separate or
 266 redundant processes. Again, the goal of implementing the JSP is to generate higher quality
 267 products that positively impact patient safety.

268 In addition to organizational leadership, various members of the organization have a shared
 269 responsibility for product security and thus benefit from the implementation of the JSP. For
 270 example, a vendor may share its evaluation of maturity against the JSP with customers. The
 271 vendor may also share this information with the HSCC with the intent of informing future
 272 iterations of the JSP. Additional granularity regarding stakeholder roles and responsibilities as
 273 well as potential organizational structures for implementing security are found in Appendix C
 274 and Appendix H respectively.

275 Organizations adopting this framework should consider providing existing personnel with
 276 necessary training to achieve focused incorporation of cybersecurity expertise (see Appendix I

277 for additional granularity regarding on organizational training). Maintaining functional
278 competency can best be achieved by establishing a routine training regimen or periodic re-
279 assessment of need.

280

281 **VII JSP Product Security Framework Implementation**

282 This section expands and articulates on security activities and processes in the JSP framework
283 (see Figure 1) in the context of where they align with traditional quality systems processes, and
284 cross references appendices with applicable examples and templates. The goal in adopting the
285 JSP is to integrate the security activities and processes in the JSP framework into existing
286 processes where applicable. For additional information regarding the authoritative sources that
287 were used to draft the content that follows, please see Appendix D.

288 **A. Risk Management**

289 Product security risk assessment is an integral component of overall product risk management.
290 There are specific considerations necessary for ensuring cybersecurity risks identified during
291 design, development, or post launch complaint handling are properly analyzed, evaluated, and
292 documented. This section describes risk management from product concept through product
293 launch.

294 **i. Risk Register**

295 A risk register, also referred to as a risk log, may be standalone or multiple repositories,
296 which can be used to report on efforts across the framework activities, track remediation,
297 and map new known vulnerabilities or potential risks. For vendors, the risk register will
298 be populated from product portfolio management and information from the cybersecurity
299 management plans as described below. Customers also benefit from maintaining a risk
300 register based on information from customer security documentation (see Section VII,
301 Design Control, subsection vi(b) for a description of customer security documentation)
302 and vulnerability disclosures from vendors.

303 **ii. Cybersecurity Management Plan**

304 Beginning at the concept phase, a plan is created to establish how cybersecurity will be
305 managed throughout the product lifecycle of the vendor's product. This plan is
306 maintained throughout the product lifecycle and includes:

- 307 • Reports for product security risk assessment, penetration testing, static code
308 analysis, and vulnerability scanning
- 309 • Documentation of secure coding standards and system hardening standards
310 applied during development and at installation
- 311 • Plans for incident management, vulnerability management, and patch
312 management
- 313 • Documentation of service, remote support, and decommissioning procedures
314 which may also be reflected in service contracts
- 315 • Customer security documentation that is ready for customer distribution
- 316 • Documentation of exceptions (see Section VII, Compliant Handling and
317 Reporting, subsection v for a description of exceptions)

318 This management plan should be cross-functionally reviewed and approved by business
319 leadership in a vendor’s organization. Components of this plan necessary for operation
320 and management of product security are provided to customers by inclusion in customer
321 security documentation, user manuals, and reflected in contractual agreements between
322 the vendor and customer.

323 **iii. Product Security Risk Assessment**

324 **Product Inventory**

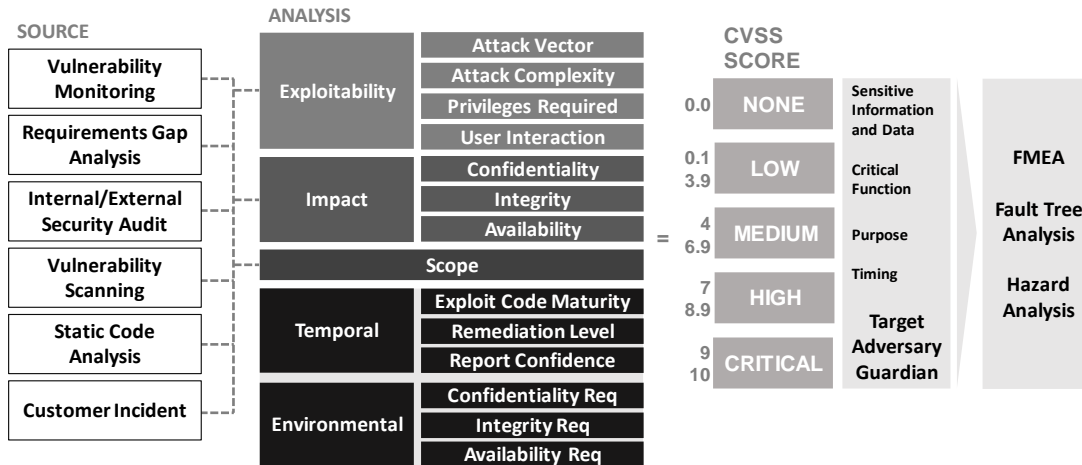
325 Document and maintain a comprehensive list of all software enabled products, product
326 versions, solutions, and services commercially available, in support or in development, in
327 order to track cybersecurity risks.

328 Security risk assessment may be performed as part of or separately from other types of
329 risk assessment, including those described in ISO 14971. The objective of risk
330 assessment for known vulnerabilities or potential cybersecurity risks is to determine the
331 comprehensive impact, for example, to clinical safety, business operations, intellectual
332 property, patient privacy, contractual requirements, regulation, and law. The risk
333 assessment will also enable the risks and vulnerabilities to be prioritized for response.
334 Figure 2 is an example of: the sources from which a known vulnerability may be
335 identified; the analysis categories used to score the vulnerability; and the output of the
336 risk assessment. Risk assessments should reflect the target operational environment and
337 use case of the product.

338 Known common vulnerabilities and exposures (CVEs) identified in design and
339 development or during complaint investigation of a launched product are analyzed and
340 evaluated using a consistent vulnerability scoring methodology. One methodology that
341 may be leveraged is the common vulnerability scoring system (CVSS). If CVSS is used,
342 the latest version available should be used at the time of risk assessment to derive the
343 level of cybersecurity risk and information that may be further used in preliminary hazard
344 analysis (PHA), failure mode and effects analysis (FMEA), or other risk assessment tools
345 not specific to cybersecurity, as indicated in Figure 3. Utilizing the most recent version
346 of CVSS can help in this analysis and avoid challenges with determining exploitability
347 for security risks. For many vulnerabilities, CVSS scoring may already be provided based
348 on original equipment manufacturer (OEM) or industry evaluation, but it is recommended
349 that CVSS is calculated specific to the product’s implementation with consideration for
350 worst case scenarios where implementation is not strictly controlled (See Appendix J for
351 more information on a draft CVSS rubric for the healthcare context which may aid in this
352 assessment).

353

354

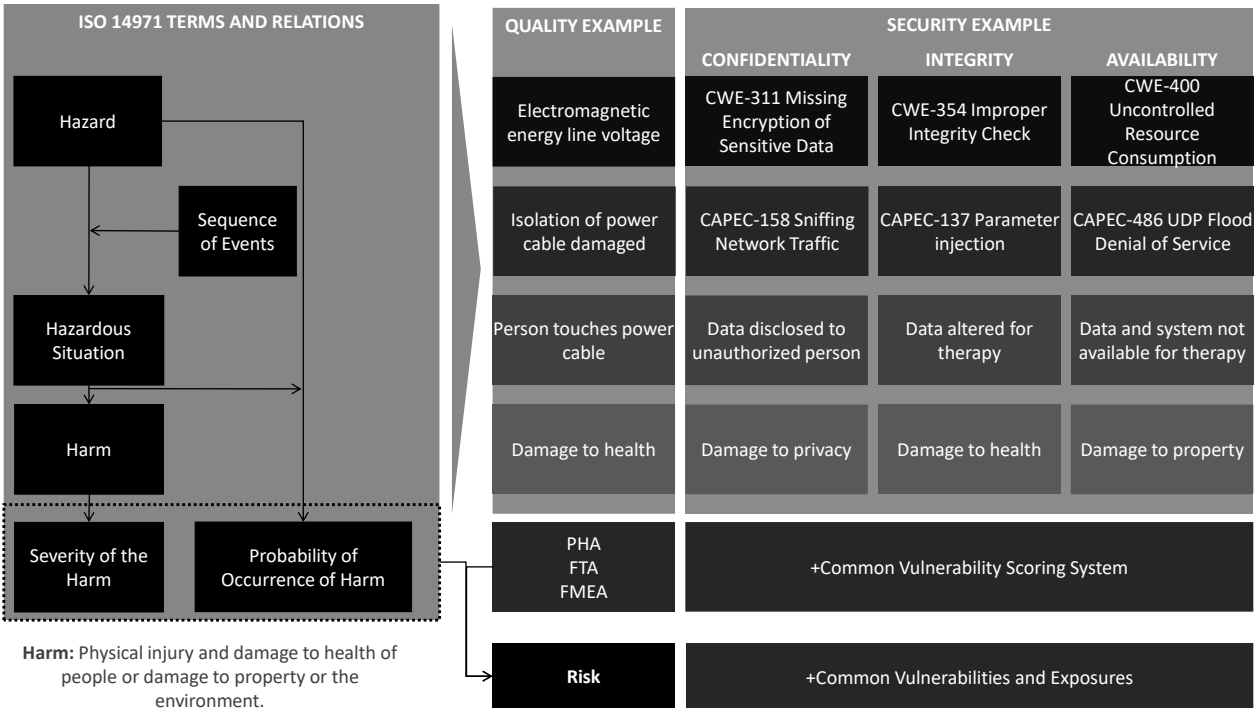


355
 356 **Figure 2. Risk Assessment Sources.** Assessing risk from different sources and generating
 357 severity scoring that may be used in safety-related risk assessment.

358
 359 As it relates to Figure 2 above:

- 361 • None to low risk means negligible or no impact to confidentiality, integrity, or
 362 availability of the patient, user, vendor or customer environment (environmental)
 363 which may be considered controlled risk.
- 364 • Medium to high risk means potential known vulnerabilities that may result in
 365 adverse events impacting confidentiality, integrity, or availability to the patient,
 366 user, vendor or customer environment which otherwise may be considered
 367 uncontrolled risk depending on impact to safety and efficacy.
- 368 • Critical risk introduces potential for injury or harm to patients or users of products
 369 including impact to sensitive information and data or critical functions which
 370 otherwise may be considered uncontrolled risk.

371



372
373 **Figure 3. Risk Assessment Mapping.** Illustration of how a safety-related risk management
374 process maps to a security-related issue for medical technology

375 **iv. Additional Risk Management Areas**

376 **Supply Chain**

377 Secure, according to a vendor information security policy, development and
378 manufacturing environments such that additional security risk is addressed prior to
379 deployment of a product to a customer. These measures should include malware
380 protection measures, file system integrity checking, and access control for intellectual
381 property during the supply chain process.

382 **Third-Party Entities**

383 It is important that external entities involved in the product lifecycle of a medical device
384 or healthcare information technology ensure applicable components described in the JSP
385 framework (Figure 1) can be achieved. Furthermore, by undergoing routine assessment
386 against the applicable components of this framework, third-party entities demonstrate
387 their commitment to further bolstering the state of medical device and health IT security.
388 Additional granularity is provided in an example of a third-party security agreement in
389 Appendix F.

390 **B. Design Control**

391 Design controls consist of policies and procedures that ensure that product design inputs are met
392 so that correct requirements can be developed. For cybersecurity, organizations apply applicable
393 standards and testing to software code during product development as well as during each
394 software release. These design control principles also apply to components provided by third-
395 parties that are used in finished products. The section that follows describes components of the

396 JSP security framework relevant to design control from product concept through product
397 qualification.

398 **i. Design Input Requirements for Security**

399 As a subset of design input requirements, establish high-level security requirements based
400 on: authoritative sources for security standards and best practices; a vendor's own
401 security requirements when they verifiably exceed existing standards; regulatory
402 requirements for security of technology or medical technology specifically, and customer
403 feedback relating to security. These requirements should be assessed for applicability to a
404 product during the design and development processes (Figure 1). Additional specifics
405 regarding some of these requirements are found in Appendix E. It is expected that
406 additional information regarding cybersecurity vulnerabilities may be obtained once the
407 product is launched. As a result, it is important to incorporate known cybersecurity
408 vulnerabilities and relevant compensating controls into the design control process (i.e.
409 into design control policy and procedures).

410 **ii. System Requirements, System Hardening Standards, and Vulnerability**
411 **Scanning**

- 412 • Identify, apply and maintain system hardening standards provided by a third-party
413 component vendor or an authoritative source for securely configuring all products
414 and components used in a vendor product. See Appendix D for examples of
415 authoritative sources for standards and testing.
- 416 • Perform vulnerability scanning periodically throughout product development and
417 conduct automated testing to ensure secure system configuration and patching.

418 **iii. Software Requirements, Secure Coding Standards, and Code Analysis**

- 419 • Apply secure coding standards during the development of software that outline
420 secure coding practices generic to any programming language, and language-
421 specific secure coding standards specific to a programming language.
- 422 • Perform static and dynamic code analysis periodically throughout product
423 development testing and integrate automated solutions into development tools to
424 ensure secure coding standards are followed.

425 **iv. Patch Management Requirements**

426 Routinely identify, apply and maintain system-patching throughout the product
427 development process for products and components, including those provided by third-
428 parties. Consider remediation planning within a reasonable timeframe - including an
429 upgrade of the products and components - if patches are no longer supported by their
430 third-party vendor. The deployment and application of patches will have a defined time
431 of disruption to system operation and minimal impact on availability for patient care. See
432 Section VII, Complaint Handling and Reporting, subsection vi for additional granularity
433 on vulnerability and patch management once the product is launched.

434 **v. Security Testing**

- 435 • Conduct robustness testing during unit and integration testing of proprietary
436 software in development; test interfaces such as user interfaces, network
437 protocols, and file inputs for ability to withstand and handle potentially malicious

438 input, as well as denial of service attacks and events; and apply standard IT
439 practices such as vulnerability scanning.
440 • Conduct penetration testing. It is paramount that an independent entity trained
441 and/or certified in cybersecurity verifies cybersecurity testing performed and
442 security controls implemented during design control, as well as in each software
443 release near or at completion of risk remediation. Additionally, they may apply
444 custom cybersecurity testing methodologies based on threat modeling to ensure
445 comprehensive use case coverage. Based on product complexity, connectivity,
446 and integration with customer environments and reliance on customer security
447 controls, a penetration test is recommended on the product in its deployed
448 configuration prior to customer use. Documentation by the vendor of penetration
449 testing reports is critical to include in product design documentation and the
450 cybersecurity management plan; include unmitigated findings in customer
451 security documentation.

452 **vi. Customer Security Requirements**

453 **a) Service and Support Access**

454 When remotely or locally accessing customer systems, it is critical that a vendor
455 maintain permissible security and privacy controls and adhere to customer
456 information security policies. Support tools and processes should be monitored
457 for vulnerabilities and insecure practices. The vendor is responsible for providing
458 customer security documentation which comprehensively describes the control
459 measures implemented. In particular, vendor service and support personnel in
460 collaboration with customers are responsible for:

- 461 • Obtaining consent from the customer prior to accessing customer
462 environments in addition to uniquely identifying service and support
463 personnel upon authentication and authorization to a system. Also, document
464 processes for how and when local and remote access is performed for service
465 and support.
- 466 • Avoiding inclusion of any credentials in product information documentation
467 such as service manuals, which may allow unauthorized access to the product.
468 Default passwords or credentials may be documented when instructions are
469 provided to make those credentials unique.
- 470 • Ensuring system cybersecurity controls are always returned to intended
471 configuration prior to completing any vendor service and support visit.

472
473 In addition:

- 474 • Credentials and passwords should be unique, changed on a regular basis and
475 immediately removed or changed following any service personnel
476 termination.
- 477 • Remote access should be done using some type of multi-factor authentication.
- 478 • Customer data, including patient data, may never leave the site without
479 written consent and approval from the customer. Data should be de-identified
480 when possible and a clear communication of use of the data must be provided.
- 481 • Any use of removable media should be approved by customers and customer
482 information security policies should be adhered to before utilization.

- 483
- 484
- 485
- 486
- 487
- 488
- 489
- 490
- 491
- 492
- 493
- 494
- Decommissioning or transfer of products and components from a customer facility, or removal for refurbishment, requires any sensitive information and data to be destroyed or transferred with reasonable and appropriate safeguards with the customer’s written authorization.
 - Customers may accept responsibility to destroy sensitive information and data from any product if they wish to do so. Clearly document and follow any federal and local regulatory or legal procedures for transfers of this data.
 - Service may determine approved methods for managing sensitive information and data. In accordance with customer data retention requirements, the destruction of this data must be clearly documented and follow any local regulatory or legal procedures.

495 **b) Customer Security Documentation**

496 For any commercialized product, it is critical that the vendor develop and

497 maintain documentation which describes all pertinent security information related

498 to the product. Furthermore, customer security documentation needs to be

499 updated when significant changes occur in existing or new product versions. This

500 documentation is prepared for external distribution and consumption by

501 customers. Customers, in turn, are responsible for processing vendor-provided

502 customer security documentation to complete questionnaires, agreements, and/or

503 risk assessments during product procurement phases and incorporating results into

504 a risk management platform as well as an asset management platform for ongoing

505 management.

506 Customer security documentation provided by vendors includes:

- 507
- 508
- 509
- 510
- 511
- 512
- 513
- 514
- 515
- 516
- 517
- 518
- 519
- 520
- 521
- 522
- 523
- All components provided or required for use, also known as a bill of materials, using the common platform enumeration convention and major version number. This would include components such as software (commercial and open source) and firmware required for device operation
 - Description of secure configuration
 - Data flow diagrams that capture items flowing in and out of the device, open network ports and active services, as well as any requirements for network connectivity
 - Remote access methods and tools, if used
 - Access control design including privileged access controls and vendor maintenance and/or service accounts
 - Comprehensive description of the control measures implemented
 - Patch management plan developed by the vendor that identifies any customer responsibility as part of the plan
 - Required cybersecurity controls including malware protection that supported the vendor risk assessment
 - Logging and audit capabilities to support customer security operations

- 524 • Assumptions and requirements at installation and in use to maintain security
- 525 • Summary of known security risks and considerations, including unmitigated
- 526 findings from penetration testing
- 527 • Contact information for the vendor to report incidents, vulnerabilities, or for
- 528 general inquiries regarding security
- 529 For context regarding what may be included in customer security documentation
- 530 and what it might look like, see Appendix G.

531 **C. Complaint Handling and Reporting**

532 Gathering feedback on the cybersecurity performance of their products post product launch is
533 important for vendors, and complaints are a mechanism for obtaining this feedback. The section
534 that follows provides insight into the types of information vendors may receive and actions they
535 may take as a result.

536 **i. Customer Complaint Escalation**

537 Customer complaint evaluation or investigation by the vendor includes steps to determine
538 if there is a product-related cybersecurity vulnerability or incident. A cross-functional
539 team may be assembled to ensure a coordinated investigation and appropriate response.
540 Specifically, the investigation includes close coordination with the affected customers
541 and appropriate parties. Ensure effective escalation and triage by having adequate
542 procedures and classification for potential cybersecurity issues for handling by service
543 and support. Customers and vendors should perform timely information sharing during an
544 investigation to support rapid response.

545 If the customer product complaint is associated with protected health information or
546 personally identifiable information, then privacy considerations must be accounted for
547 (e.g. privacy notifications, breach investigation) and other potentially affected customers
548 must be notified. The vendor should provide information needed for proper incident
549 response to enable successful breach determinations.

550 If the complaint is associated with vendor managed or owned assets but not a vendor
551 product, such as a service laptop or removable media, then upon receiving the complaint
552 the vendor will inform its information security organization. Depending on the type of
553 incident, notification of privacy or compliance officers may be needed as well. Additional
554 responses may also be needed that include customer or regulatory notification.

555 Risk assessment and remediation planning is an integral part of the complaint
556 investigation. As a part of this assessment, product cybersecurity risks are documented in
557 service and support complaint handling systems in addition to risk management files.
558 Remediation may include advised compensating controls and fixes as appropriate.

559 **ii. Reporting Considerations**

560 In the interest of strengthening cybersecurity within the medical technology ecosystem, it
561 is essential for vendors to communicate cybersecurity vulnerabilities to appropriate
562 stakeholders. In addition to vendor customers, these stakeholders include Cyber
563 Emergency Response Teams (CERTs) and groups that share medical technology
564 vulnerability and threat information (e.g. information sharing and analysis organizations).

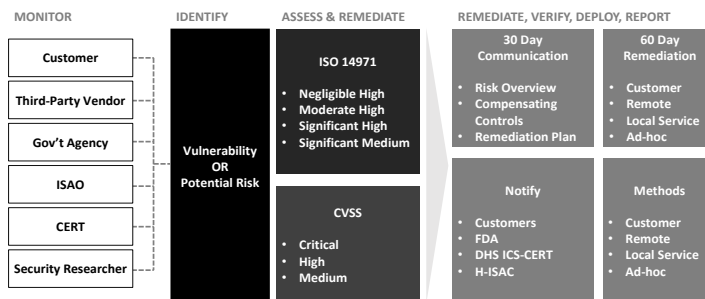
565 Vendors should also be aware of any additional reporting and remediation requirements
 566 imposed by regulators in the jurisdictions in which they operate (e.g. FDA guidance on
 567 Postmarket Management of Cybersecurity in Medical Devices for medical device
 568 manufacturers marketing product in the US), as these vulnerabilities may pose patient
 569 safety concerns.

570 **iii. Security Incident Management, Response and Communication**

571 Provide timely responses and communications to all stakeholders impacted by
 572 vulnerabilities and incidents for commercialized products as described below.

- 573 • Manage internally reported issues within 30 days of initial discovery and the
 574 designated cross-functional team provides an update of the issue status to internal
 575 stakeholders and governance every 60 days thereafter until closure.
- 576 • Produce targeted customer bulletins or notifications and post to a public webpage
 577 or deliver via other available mechanisms to customers within 30 days of initial
 578 discovery for customer and third-party reported issues. Evaluate related customer
 579 security documentation to determine if updates are indicated; if deemed
 580 necessary, proceed to update. Provide status updates to customers and third-
 581 parties reporting vulnerabilities and incidents with a routine cadence established
 582 by the cross-functional team while complaint handling investigation is in
 583 progress. Achieving the aforementioned timing for bulletins or notifications by
 584 the vendor during incidents may be dependent on timely and accurate
 585 communication with customers.
- 586 • Coordinate vulnerability disclosures with a Cyber Emergency Response Team
 587 (CERT) and Information Sharing and Analysis Organization (ISAO) recognized
 588 by the FDA. For an overview of vulnerability disclosure terms, definitions,
 589 concepts, guidelines, and benefits please see the international standard and white
 590 paper referenced under “Security Incident Response and Communication” in
 591 Appendix D. Though out of scope for this document, other reporting such as that
 592 required by federal (e.g. the Health Insurance Portability and Accountability Act
 593 (HIPAA)) and state laws, regulatory compliance etc. may be needed. Figure 4
 594 below is an example of a coordinated vulnerability disclosure process.

595



596
 597 **Figure 4. Example coordinated vulnerability disclosure process.** Organizations obtain
 598 vulnerability information by monitoring various sources. Subsequently a potential vulnerability
 599 is identified, assessed, verified, remediated, and communicated as appropriate.

600 **iv. Remediation Planning**

601 Throughout design and development, a product security risk assessment is necessary to
602 determine the level of risk and subsequent actions for security requirements including
603 remediation planning. Below is an example of how low, medium and high risks can be
604 managed.

- 605 • Low risk can be addressed or accepted as is and documented as an exception (see
606 following section to learn more about exceptions)
- 607 • Medium to high and critical risk can be addressed as requirements for design
608 input and mitigated accordingly
- 609 • Routine vulnerability and patch management may be addressed continuously

610 For commercialized products, security risk assessment and remediation planning is
611 performed as part of a post market management (post-launch) process.

- 612 • Low risks may be addressed separately in a reasonable amount of time, but at
613 minimum during the next product or software update
- 614 • Recommendations for medium to high and critical risks, which may align with
615 uncontrolled risks per FDA’s guidance Postmarket Management of Cybersecurity
616 in Medical Devices, include communicating with the customer and user
617 community about the vulnerability, identifying the devices which could
618 potentially be impacted and providing interim control measures to mitigate risk as
619 well as a remediation plan within 30 days of learning of the vulnerability. Patches
620 must be available with at least one of the deployment methods promptly and
621 within a maximum of 60 days after learning of the vulnerability. As soon as
622 possible but no later than 60 days after learning of the vulnerability, the
623 manufacturer fixes the vulnerability, validates the change, and distributes the
624 deployable fix to its customers and user community such that the residual risk is
625 brought down to an acceptable level.
- 626 • Risks which have resulted in an incident where unauthorized disclosure of PHI or
627 PII will require data breach investigation and potential notification to customers
628 in accordance with local laws and regulation. Other sensitive information and
629 data such as intellectual property will require data breach investigation and
630 potential notification to stakeholders.

631 Corrective and preventive action plans (CAPA) are established in compliance
632 with vendor CAPA policy/procedure in order to evaluate the need to correct
633 existing or potential quality issues that impact the security of products and to
634 develop actions to prevent their occurrence or recurrence.

635 **v. Exceptions**

636 An exception is an instance when a cybersecurity risk is identified (both pre- and post-
637 launch of the product) and the vendor determines that no action is needed. As is
638 appropriate in all cases, it is important for the manufacturer to document the risk in the
639 product’s design history file and/or risk management files. For risks documented as
640 exceptions that require compensating controls to reduce the risk to none-to-low risk, a
641 description of the risk and the compensating controls, including associated procedures,
642 should be provided in customer security documentation for the product.

643 **vi. Vulnerability Management and Patch Management**

644 Prior to commercialization, a vendor establishes a cybersecurity management plan to
645 identify, evaluate, and respond to any cybersecurity incident or vulnerability including
646 known and zero-day vulnerabilities. The plan would not be complete without addressing
647 routine patching throughout the product lifecycle. Standardizing a pre-determined
648 frequency for patches and updates is recommended, with a quarterly frequency at
649 minimum. Publishing and coordinating patches in a timely manner so as to mitigate
650 medium to high risk vulnerabilities is of prime importance to any vulnerability and patch
651 management program. Critical elements of a vulnerability and patch management plan
652 include the ability to:

- 653
- 654 • Continuously monitor, track, and plan for cybersecurity incidents, vulnerabilities,
655 upstream patches, and end of support dates from predefined sources based on
656 inventory of firmware, software, communication modules, etc. Products and
657 components (including those contracted components provided by third-party
658 entities) may also be a source of vulnerabilities and should similarly be subject to
659 monitoring
- 660 • Determine the level of risk and subsequent actions necessary to mitigate
661 cybersecurity risks by using product risk assessment, remediation planning and
662 product security risk assessment. In particular, document cybersecurity risks in
663 defect, bug, or issue tracking systems or product backlog, in addition to design
664 history files and/or risk management files
- 665 • Validate the remediation and successful patching of vulnerabilities, including
666 impact to performance and clinical use
- 667 • Perform proper version controlling to ensure patches can be identified once
668 deployed on products
- 669 • Identify capabilities necessary for customers and vendors to determine if a
670 security incident has occurred from any exploited vulnerability
- 671 • Deploy remediation, including routine and emergency software patches, by
672 implementing at least one of the following secured methods that are then
673 documented by both vendor and customer:
 - 674 ▪ Remote Update: Patches applied via secure authorized remote service and
675 support platforms provided by the vendor
 - 676 ▪ Customer Administered: Validated patches will be made available for
677 customer retrieval and installation from a designated source including
678 direct download from the third-party that provides the product or
679 component
 - 680 ▪ Service Visit: Local service administered cybersecurity patches. Note that
681 this method is less optimal due to the time required to deploy local service
682 personnel to customer facilities. However, it has utility in cases where
683 faulty patching has foreseeable and serious safety risk and local service
684 personnel may be required for resolution
 - 685 ▪ Ad-hoc Patching: Customers may accept engineering and technical risk
686 for all other deployment mechanisms and/or application of cybersecurity
687 patches not validated by the vendor. Note that this method is not advised
688 due to the lack of validation by the vendor and potential impact to system
689 performance or patient safety

- 690 • Make customers aware of the availability of cybersecurity patches and upgrades
691 for products through a public webpage and/or direct customer notification (e.g.,
692 email followed by letter).
 - 693 ▪ For vendor-managed remote updates and service visits, routine reporting
694 to customers of failures to patch products in the field is necessary,
695 including products and components provided by third-party entities that
696 are no longer supported by their vendor
 - 697 ▪ It is essential that customers establish processes and/or technical means for
698 routinely monitoring the designated communication channels predefined
699 by the vendor for new information or changes regarding patches

701 **vii. End of Life/ End of Support and Decommissioning**

702 The cybersecurity management plan incorporates consideration for appropriate actions
703 for the vendor and its customers when security for the product can no longer be supported
704 or when the vendor discontinues support and maintenance of the product.

- 705 • Consideration for end of support includes when third-party products and
706 components are no longer supported by their manufacturer or developer and when
707 known common vulnerabilities and exposures are identified but not remediated by
708 the third-party component manufacturer or developer. Provide anticipated end of
709 life and end of support dates to customers as part of customer security
710 documentation.
- 711 • For commercialized products that will receive an end of life or end of support date
712 for the first time, a reasonable amount of advanced notification is recommended
713 so that customers can take any necessary action including removal of network
714 connectivity, transition to a supported product, and implementation of
715 compensating controls provided by the vendor as part of end of life and end of
716 support. At a minimum, 3 years is considered a reasonable amount of time
717 between communicating and making effective end of life or end of support.
- 718 • Customers should be aware of the end of life and end of support dates for systems
719 in their inventory and make risk-based decisions on their replacement or
720 continued use. If intending to replace, organizations can develop
721 replacement/upgrade plans for each system. If the decision is continued use
722 beyond the end of life and end of support dates, the customer is advised to
723 perform a risk assessment to determine risk reduction strategies it can perform
724 independently, which may include network segmentation, isolation, system
725 hardening, or other defense-in-depth strategies.

727 **VIII Evaluating JSP Progress and Maturity**

728 **A. Evaluating Progress**

729 An organization involved in the design, development, production, deployment, service, and
730 support of medical device and healthcare information technology may establish means for
731 achieving each of the applicable plan components with target dates and periodically assessing
732 progress and maturity against the JSP. The table below is an example of a JSP maturity
733 assessment. Once the framework is understood, it is recommended that an initial assessment is

734 completed and the follow-ups scheduled and executed. Note that other maturity assessments may
 735 be of value and additional information on the CMMI maturity assessment is found in Appendix
 736 K.

737

Plan Component	Description	Current Maturity	Target Maturity	Milestones
----------------	-------------	------------------	-----------------	------------

Organization

Structure	<p>Does the organization have a Chief Product Security Officer?</p> <p>Does the organization have a product security function?</p> <p>Are the product security functions roles & responsibilities clearly defined?</p> <p>Is the product security function staffed appropriately?</p>	[1-5]	[1-5]	[YYYY/MM]
------------------	---	-------	-------	-----------

Governance	<p>Are there existing policies and/or procedures that cover product security?</p> <p>Has organizational leadership approved of the product security policy and procedures?</p> <p>Is the organization audited against product security policies/procedures? How frequently?</p> <p>Are product security metrics briefed to leadership such as Chief Quality Officer, Chief Medical Safety Officer, R&D leadership, etc.? If so, how frequently?</p>			
-------------------	---	--	--	--

738

Risk Management

Risk Register	Has an inventory of products been created for	[1-5]	[1-5]	[YYYY/MM]
----------------------	---	-------	-------	-----------

Risk Assessment	<p>commercialized products and products in development?</p> <p>Are security risks tracked in R&D defect tracking systems, design history or risk management files?</p> <p>Are security risks tracked in service complaint handling systems or risk management files?</p>			
	<p>Is there an established method used for security risk assessment?</p> <p>Have policies and procedures been updated to incorporate security risk assessment and triage to other types of risk assessment?</p>			
Supply Chain	<p>Are development and manufacturing environments assessed and managed for adherence to information security policy?</p>	[1-5]	[1-5]	[YYYY/MM]
Third-Party Entities	<p>Have third-parties been assessed against the components of this framework?</p> <p>Are third-parties routinely assessed for security?</p> <p>Does the organization have security requirements in the contract language for suppliers and third-parties?</p>			
Exceptions	<p>Are exceptions to framework components documented in design history and/or risk management files?</p> <p>Are compensating controls associated with exceptions provided in customer security documentation?</p>			

Design Control				
Design Input Security Requirements	Are cybersecurity requirements incorporated in design input for products in development?	[1-5]	[1-5]	[YYYY/MM]
Standards and Testing	<p>Are system hardening standards, system patching, and vulnerability scanning incorporated in product development practices?</p> <p>Are secure coding standards and code analysis incorporated in product development practices?</p> <p>Is security testing such as penetration testing performed by trained cybersecurity professionals during design control?</p> <p>Is robustness testing performed during product development?</p>			
Vulnerability Management & Patch Management	<p>Have processes been instituted to monitor, identify, assess, remediate, and validate security patches for product software and third-party components?</p> <p>Are validated patches deployed using an established method?</p> <p>Can reports be generated to show patching failures?</p> <p>Is there a public webpage where customers can go to identify new patches?</p>			
Customer Requirements	Do service and support personnel have procedures for requesting access to customer			

Cybersecurity Management Plan	<p>systems and restoring security measures?</p> <p>Are controls in place for service personnel to uniquely authenticate to customer systems?</p> <p>Is there established policy and procedures around the use of removable media with products and handling of customer data?</p>			
	<p>Are plans in place to maintain security throughout the lifecycle of a product?</p> <p>Do products have anticipated end of life and/or end of support dates established with consideration to supporting third-party products and components?</p>			
Complaint Handling				
Customer Complaint Escalation	<p>Do escalation procedures define cybersecurity signals?</p> <p>Are customer reported cybersecurity issues documented in complaint handling systems?</p> <p>Are processes in place to ensure review of reported complaints related to cybersecurity?</p>	[1-5]	[1-5]	[YYYY/MM]
	Reporting Considerations	<p>Have processes been established to notify a CERT, ISAO, and/or regulator as appropriate of reported cybersecurity issues?</p>		
Security Incident Management, Response and Communication	<p>Are internal teams engaged within 30 days of a reported security incident and updated every 60 days thereafter?</p>			

Remediation Planning	Are the incident response processes regularly practiced?			
	Is there a public webpage where bulletins or advisories relating to vulnerabilities or incidents can be posted?			
	Are there clearly defined criteria for remediation of security risk for products in development?			
	Are there clearly defined criteria for remediation of security risk for commercialized product?			
	Are medium to critical vulnerabilities communicated to customers within 30 days?			
	Are medium to critical vulnerabilities remediated within 60 days?			

739 **B. Maturity Levels**

740 The following levels are used to describe the state of maturity for individual components of the
741 Joint Security Plan. In order to move to a higher maturity level, all the elements of previous
742 levels should be satisfied.

743 **Level 1: Initial**

744 One or multiple framework components have been presented to internal stakeholders
745 and plans have been drafted, but there is no proven or formalized process nor people
746 responsible.

747 **Level 2: Managed**

748 Framework components have been planned and execution is underway. The
749 established plans ensure framework components are performed, measured, and
750 controlled with routine visibility provided to management.

751 **Level 3: Defined**

752 All of the framework components have been achieved. Formal policies and
753 procedures have been established as well as incorporated in quality management
754 systems. Internal stakeholders have been provided clear description of activities and
755 are provided training. Deliverables for the framework component are well
756 documented and routinely reviewed among internal stakeholders.

757 **Level 4: Quantitatively Managed**

758 All aspects of a framework component are achieved and various performance metrics
759 are collected to determine areas of improvement. The following are performance
760 metrics that may be considered:

- 761 • Number of reported security complaints
 - 762 ▪ Average response time to customers
 - 763 ▪ Average time to closure for security complaints
 - 764 ▪ Average time to customer communication
- 765 • Number of cybersecurity defects out of design control
 - 766 ▪ Average time to remediation
- 767 • Percentage of patches successfully applied remotely to deployed product
- 768 • Percentage of patches successfully applied by customers to deployed product
- 769 • Percentage of patches successfully applied by service to deployed product
- 770

771 **Level 5: Optimizing**

772 Metrics collected on a framework component are routinely reviewed and process
773 improvement plans are established. Quantitative process improvement objectives are
774 established and continuously revised to reflect changes to industry standards and the
775 JSP. Review of quantitative analysis produces predictable results. Process variation
776 across multiple products is understood and when variation produces under-
777 performance it is addressed through the creation of process improvement plans with
778 cross-functional ownership. The process of continuous improvement is intrinsic to all
779 those involved in the design, development, production, deployment, service, and
780 support of medical device and healthcare information technology.
781

782 **Appendix A: Acronyms**

783 This appendix section provides an overview of the acronyms used in this document.

784	C-I-A	Confidentiality Integrity Availability
785	CISO	Chief Information Security Officer
786	DHS	U.S. Department of Homeland Security
787	EHR	Electronic Health Record
788	EU	European Union
789	FDA	U.S. Food and Drug Administration
790	GDPR	General Data Protection Regulation
791	HDO	Healthcare Delivery Organization
792	HCIC Task Force	Health Care Industry Cybersecurity Task Force
793	HHS	U.S. Department of Health and Human Services
794	HIMSS	Healthcare Information and Management Systems Society

795	HIPAA	Health Insurance Portability and Accountability Act
796	HPH	Healthcare and Public Health
797	IT	Information Technology
798	ISAO	Information Sharing and Analysis Organization
799	ISAC	Information Sharing and Analysis Center
800	MDM	Medical Device Manufacturer
801	NIST SP	National Institute of Standards and Technology Special Publication
802	NIS	Network and Information Systems Directive (EU) 2016/1148)
803	H-ISAC	Health Information Sharing and Analysis Center
804	NCCoE	National Cybersecurity Center of Excellence
805	NSA	National Security Agency
806	PHI	Protected Health Information
807	PII	Personally Identifiable Information
808	R&D	Research and Development
809	SDL	Security Development Lifecycle
810	SDLC	Software Development Life Cycle
811	U.S.	United States
812		

813 **Appendix B: Terminology**

814 Various cybersecurity and healthcare centric terms are used throughout this document. This
815 appendix section provides an overview of what is meant by some of these key terms. Note that
816 some of these terminologies and definitions were derived from authoritative sources listed in
817 Appendix D which describes the drafting of the Joint Security Plan.

818 **Code Analysis:** Source code analysis is the automated testing of a program’s source code with
819 the purpose of finding faults and fixing them before the software is sold or distributed.

820 **Common Platform Enumeration (CPE):** An industry standard structured naming scheme for
821 information technology systems, software, and packages.

822 **Common Vulnerability Exposure (CVE):** CVE is a list of information security vulnerabilities
823 and exposures that aims to provide common names for publicly known problems

824 **Common Vulnerability Scoring System (CVSS):** A security industry standard for prioritizing
825 the severity of security issues.

826 **Compensating Controls:** Alternative security controls employed by organizations in lieu of
827 specific controls. These are controls that provide equivalent or comparable protection for
828 organizational information systems and the information processed, stored, or transmitted by
829 those systems.

830 **Complaint Handling:** Process for receiving, reviewing, and evaluating complaints.

831 **Coordinated Vulnerability Disclosure:** The process of gathering information from
832 vulnerability finders, coordinating the sharing of that information between relevant stakeholders,
833 and disclosing the existence of software vulnerabilities and their mitigations to various
834 stakeholders, including the public

835 **Controlled Risk:** Controlled risk is present when there is sufficiently low (acceptable) residual
836 risk of patient harm due to a device’s particular cybersecurity vulnerability.

837 **Critical Functions:** Any product functionality which impacts the clinical safety or significantly
838 disrupts the business operations of Customers.

839 **Customers:** Includes healthcare providers and patients.

840 **Customer Complaint:** Complaint means any written, electronic, or oral communication that
841 alleges deficiencies related to the identity, quality, durability, reliability, safety, effectiveness, or
842 performance of a medical device or health information technology after it is released for
843 distribution.

844 **Customer Incident:** An occurrence from a customer’s use of software, products or services that
845 actually or potentially results in adverse consequences to (adverse effects on) (poses a threat to)
846 an information system or the information that the system processes, stores, or transmits and that
847 may require a response action to mitigate the consequences.

848 **Customer Security Documentation:** Security information provided to customers to enable
849 more robust risk assessments, identify configurable security controls, and allow them to better
850 protect their systems.

851 **Customer Security Requirements:** A user, or potential user, of a system’s functional and non-
852 functional requirements that achieve the security attributes of a system.

853 **Decommissioning:** The first physical process in the disposition process and includes proper
854 identification, authorization for disposition, and sanitization of the equipment, as well as removal
855 of Patient Health Information (PHI) or software, or both.

856 **Design:** A process of defining the architecture, modules, interfaces and data for a system to
857 satisfy specified requirements.

858 **Design control:** The application of a formal methodology used to conduct product development
859 activities.

860 **Design Input Requirements:** The physical and performance characteristics of a product that are
861 used as the basis for product design.

862 **Dynamic Code Analysis:** The testing and evaluation of a program by executing data in real-
863 time. The objective is to find errors in a program while it is running, rather than by repeatedly
864 examining the code offline.

865 **End of Life:** Indicates that the product is in the end of its useful life, as defined by the vendor,
866 and a vendor stops marketing, selling, or making major design changes in sustaining the product.

867 **End of Support:** A point beyond which the product manufacturer ceases to provide support,
868 which may include cybersecurity support, for a product or service.

869 **Exceptions:** An instance when a cybersecurity risk is identified (both pre- and post-launch of the
870 product) and the vendor determines that no action is needed.

871 **Failure Mode and Effects Analysis (FMEA):** A step-by-step approach for identifying all
872 possible failures in a design, a manufacturing or assembly process, or a product or service.

873 **Fuzz Testing:** A software testing technique, often automated or semi-automated, that involves
874 providing invalid, unexpected, or random data to the inputs of a computer program. The program
875 is then monitored for exceptions such as crashes, failing built-in code assertions or for finding
876 potential memory leaks. Fuzzing is commonly used to test for security problems in software or
877 computer systems and is a type of robustness testing.

878 **Harm:** Injury or damage to the health of people, or damage to property or the environment.

879 **Hazard:** Potential source of harm.

880 **Hazard Analysis:** The first step in a process used to assess risk and used to identify different
881 types of hazard.

882 **Incident Response:** Actions taken to mitigate or resolve a security incident.

883 **Internal/External Security Audit:** Review and examination of data processing system records
884 and activities to test for adequacy of system controls, to ensure compliance with established
885 security policy and operational procedures, to detect breaches in security, and to recommend any
886 indicated changes in control, security policy, and procedures.

887 **Malware:** A program that is inserted into a system, usually covertly, with the intent of
888 compromising the confidentiality, integrity, or availability of the data, applications, or operating
889 system. This includes both known and unknown (Zero Day) viruses, spyware, ransomware, and
890 other forms of malicious code that exploit vulnerable systems.

891 **Patch Management:** The systematic monitoring, identification, assessment, remediation,
892 deployment, and verification of operating system and application software code updates. These
893 updates are known as patches, hot fixes, and service packs to operating systems, third-party
894 products and components, and in-house developed software.

895 **Patient Harm:** Physical injury or damage to the health of patients, including death.
896 Cybersecurity exploits (e.g. loss of authenticity, availability, integrity, or confidentiality) of a
897 device may pose a risk to health and may result in patient harm.

898 **Patient Safety:** The prevention of harm to patients including that which may occur from
899 cybersecurity related events.

900 **Penetration Testing:** A test methodology in which assessors, using all available documentation
901 such as system design and working under specific constraints, attempt to circumvent the security
902 features of an information system.

903 **Preliminary Hazard Analysis (PHA):** A technique used in the early stages of system design. It
904 focuses on identifying apparent hazards, assessing the severity of potential accidents that could
905 occur involving the hazards, and identifying safeguards for reducing the risks associated with the
906 hazards.

907 **Product Lifecycle:** Managing the entire lifecycle of a product from inception, through
908 engineering design and manufacture, to service and disposal of manufactured products.

909 **Product Security Risk Assessment:** Overall process of risk analysis and a risk evaluation for
910 security issues found in products using impact to confidentiality, integrity, and availability to
911 patients, customers, and vendor to determine the acceptability of the risk.

912 **Remediation:** Countermeasures to reduce a cyber asset's susceptibility to cyber-attack over a
913 range of attack tactics, techniques, and procedures.

914 **Remediation Planning:** Planning of processes and actions by which organizations identify and
915 resolve threats to their system.

916 **Remote Access:** Access to a product or an organization's non-public information system by an
917 authorized user such as Service and Support communicating through an external network.

918 **Remote Support:** Support activities conducted by individuals communicating through an
919 external network (e.g., the Internet).

920 **Removable Media:** Portable electronic storage media such as magnetic, optical, and solid-state
921 devices, which can be inserted into and removed from a computing device and used to store text,
922 video, audio, and image information. Such devices have no independent processing capabilities.
923 Examples include hard disks, floppy disks, zip drives, compact disks, thumb drives, pen drives,
924 and similar USB storage devices.

925 **Risk Management:** Risk management is an integral part of the medical device product
926 development lifecycle. It is a systematic application of management policies, procedures and
927 practices to the tasks of analyzing, evaluating, controlling, and monitoring risk.

928 **Robustness Testing:** A testing methodology to detect the vulnerabilities of a component under
929 unexpected inputs or in a stressful environment.

930 **Secure Coding Standards:** Guidelines for writing software code that mitigates common
931 security flaws specific to a programming language or in general to all software.

932 **Security Incident:** An event that may indicate that a device's data and security may have been
933 compromised. This includes, but is not limited to:

- 934 • Attempts to gain unauthorized access to a system or its data
- 935 • Unwanted disruption or denial of service
- 936 • Unauthorized use of a system for the processing or storage of data
- 937 • Changes to system hardware, firmware or software characteristics without owner's
938 knowledge, instruction or consent

939 **Security Management Plan:** Used to document all framework components carried out through
940 the design process and post commercialization. May also capture technical and process gaps,
941 including exceptions. May be incorporated in a product risk management file or equivalent.

942 **Security Requirements:** A set of design-level requirements that comprise a product or other
943 commercial offerings, ensure security issues are mitigated in both software and system
944 components during design control, and are processed through Risk Management.

945 **Sensitive Information and Data:** Protected health information (PHI), personally identifiable
946 information (PII), proprietary software source code or business logic, configuration parameters,
947 user credentials, cryptographic keys, quality control and calibration results.

948 **Static Code Analysis:** The automated analysis of software code for security flaws and adherence
949 to a secure coding standard.

950 **System Hardening Standards:** A documented process or mechanism for securely configuring
951 or implementing commonly used technologies.

952 **Third-Party Entities:** External individuals and organizations such as vendor and suppliers
953 involved with products or acquisition, that collaborate at any point in the product lifecycle,
954 including acquisition, development and servicing.

955 **Threat Modeling:** Structured activity for identifying and managing threats.

956 **Threat Monitoring:** Solutions or processes dedicated to continuously monitoring systems,
957 networks and endpoints for signs of a security threat such as intrusions or data exfiltration.

958 **Threat Source:** The intent and method targeted at the intentional exploitation of a vulnerability
959 or a situation and method that may accidentally trigger a vulnerability.

960 **Uncontrolled Risk:** Uncontrolled risk is present when there is unacceptable residual risk of
961 patient harm due to inadequate compensating controls and risk mitigations.

962 **Validation:** Establishing by objective evidence that specified requirements conform with user
963 needs and intended use(s).

964 **Vendors:** Includes medical device manufacturers and health IT vendors.

965 **Verification:** Confirmation by objective evidence that the results of the design effort meet the
966 design input.

967 **Vulnerability:** A weakness in an information system, system security procedures, internal
968 controls, or implementation that could be exploited or triggered by a threat source.

969 **Vulnerability Disclosure:** Policy practiced by organizations as well as individuals regarding the
970 disclosure or publishing of information about security vulnerabilities and exploits pertaining to a
971 computer system, network or software.

972 **Vulnerability Scanning:** The automated analysis and detection of vulnerabilities such as
973 missing patches and misconfiguration in operating systems and other third-party software.

974

975 **Appendix C: Roles and Responsibilities**

976 Numerous stakeholders may leverage and benefit from the security activities and processes
977 described in this document. To provide additional context, the roles and responsibilities of these
978 stakeholders are described in this appendix section.

979 **For customer stakeholders**

980 1. **Patients:** Review security documentation provided by vendors and healthcare providers
981 for consumer products and in-home environments such that cybersecurity risks are
982 understood and managed.

983 2. **Healthcare Providers:** Assess the risk of new information systems entering their
984 facilities; manage risks over the lifecycle of these information systems, including
985 monitoring of vulnerability disclosures, maintaining patches, securing network
986 environments and enterprise systems; and provide training for their associates on their
987 roles for managing cybersecurity. Also referred to as healthcare delivery organizations
988 (HDOs).

989 **For vendor stakeholders**

- 990 1. **Medical Device Manufacturers:** Responsible for implementing security throughout the
991 design, development, and complaint handling for medical devices. In addition,
992 responsible for providing timely communication to customers in the form of product
993 security documentation, vulnerability disclosures, and the availability of security patches.
- 994 2. **Health IT Vendors:** Responsible for implementing security throughout the design,
995 development, and complaint handling for healthcare information technology. In addition,
996 responsible for providing timely communication to customers in the form of product
997 security documentation, vulnerability disclosures, and the availability of security patches.
- 998 3. **Product Security:** Creation and maintenance of policies, procedures, tooling, guidance,
999 training and awareness for product security across business units and functions. Product
1000 security will support product security risk assessments, automated security testing,
1001 penetration testing, remediation planning services for R&D and complaint handling.
- 1002 4. **Quality:** Ensures the framework is aligned and consistent with other corporate policies,
1003 as well as global regulations and standards for product development, risk management,
1004 manufacturing, and support. Quality, jointly with product security, will ensure adherence
1005 to the framework as with any other quality policy such as risk management and reporting
1006 requirements.
- 1007 5. **Research and Development (R&D):** Responsible for incorporating security in
1008 budgeting and resource planning; provides technical information for product security risk
1009 assessment; establishes design requirements in the development process and throughout
1010 the product lifecycle including post-commercialization maintainability. R&D will
1011 maintain record of security defects in accordance with the business unit quality
1012 management systems including design control and risk management procedures.
- 1013 6. **Product & Portfolio Management (PM, PPM):** Responsible for ensuring product
1014 security is incorporated in budget, resource, project, and roadmap planning activities
1015 throughout the product lifecycle.
- 1016 7. **Complaint Handling Unit:** Responsible for identifying complaints that have a product
1017 security impact and proper escalation of complaints.
- 1018 8. **Service and Support:** Ensure proper response to security incidents and events with
1019 products at customer sites, including proper documentation records as per business unit
1020 complaint handling procedures. Secure service assets, maintain validated security updates
1021 and ensure secure implementation, periodic reporting of security incident and events and
1022 security update tracking.
- 1023 9. **Business Unit and Regional Leadership:** Responsible for communication, compliance
1024 and adherence of the framework at the regional and local business levels. This may
1025 include the creation of local policies that align with and supplement where needed due to
1026 regional laws and regulation the over-arching framework.
- 1027 10. **Legal:** Provides business units with guidance on incident response, adherence to local
1028 security and privacy laws to ensure legal content meets policies.
- 1029 11. **Privacy:** Ensures the appropriate protection of data, such as information from or about
1030 our employees, our customers, and users of our products worldwide.
- 1031 12. **Regulatory:** Provides business units and product security with guidance on local
1032 security and privacy regulation, including any upcoming changes to those regulations.

- 1033 13. **Information Security:** Ensures vendor managed assets, including but not limited to
 1034 laptops, desktop computers, servers, removable media, and networks that interact with
 1035 products align and adhere to the vendor information security policy.
 1036 14. **Third-Party Entities:** Adhere to requirements in the framework and vendor information
 1037 security procedure. Document any exceptions in design history and/or risk management
 1038 files.

1039

1040 **Appendix D: Drafting of the Joint Security Plan**

1041 The intent and purpose of this appendix section is to outline and explain the drafting process and
 1042 authoritative sources used to address traceability to US and International standards for the
 1043 Medical Device and Health IT Joint Security Plan.

1044 In November of 2017, with facilitation by the Healthcare Sector Coordinating Council (HSCC),
 1045 an initial draft of the Joint Security Plan was developed by a group of medical device
 1046 manufacturers, health IT vendors, and FDA representatives.

1047 In February of 2018, through the Health Information Sharing and Analysis Center (H-ISAC) and
 1048 HSCC, a group of healthcare providers was invited to participate in the drafting process of the
 1049 Joint Security Plan.

1050 Following the review by medical device manufacturers, health IT vendors, and healthcare
 1051 providers, the HSCC invited government and policymakers to provide feedback and promote use
 1052 of the Joint Security Plan among all stakeholders referenced in the document.

1053 There are many different authoritative sources which were used to develop and/or can be used to
 1054 achieve aspects of the Joint Security Plan. The following is a list of those sources and the
 1055 associated section in the Joint Security Plan:

1056

1057

JSP Framework Overview	
Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients publication	https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf
Risk Management	
AAMI TIR 57	http://www.aami.org/productspublications/ProductDetail.aspx?ItemNumber=3729
IEC 80001-1	https://www.iso.org/standard/44863.html
NIST CSF	https://www.nist.gov/cyberframework
An Introduction to Computer Security: the NIST Handbook	https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-12.pdf

ISACA Risk IT Framework for Management of IT Related Business Risks	http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/default.aspx
ISO 14971:2007 Medical devices -- Application of risk management to medical devices	https://www.iso.org/standard/38193.html
Risk Assessment	
Common Vulnerability Scoring System	https://www.first.org/cvss/user-guide
NIST Special Publication 800-30 Revision 1.0 2012 Guide For Conducting Risk Assessments	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
Design Control	
Content of Premarket Submissions for. Management of Cybersecurity in. Medical Devices	https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf
UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	https://standardscatalog.ul.com/standards/en/standard/2900-1_1
UL 2900-2-1 Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems	https://standardscatalog.ul.com/standards/en/standard/2900-2-1_1
NIST SP 800-160 Systems Security Engineering. Considerations for a Multidisciplinary Approach in the. Engineering of Trustworthy Secure Systems	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf
Catalog of Control Systems Security: Recommendations for Standards Developers	https://ics-cert.us-cert.gov/sites/default/files/documents/CatalogofRecommendationsVer7.pdf
Secure Architecture Design	https://ics-cert.us-cert.gov/Secure-Architecture-Design
NIST Cybersecurity Practice Guide SP 1800-8, Wireless Infusion Pumps	https://nccoe.nist.gov/sites/default/files/library/sp1800/hit-infusion-pump-nist-sp1800-8a-draft.pdf
NIST SPECIAL PUBLICATION 1800-8B Volume B:	https://nccoe.nist.gov/sites/default/files/library/sp1800/hit-infusion-pump-nist-sp1800-8b-draft.pdf

Approach, Architecture, and Security Characteristics	
Secure Software Development Life Cycle Processes	https://www.us-cert.gov/bsi/articles/knowledge/sdlc-process/secure-software-development-life-cycle-processes
OWASP Security By Design Principles	https://www.owasp.org/index.php/Security_by_Design_Principles#Security_principles)
Standards and Testing	
DISA Security Technical Implementation Guides	https://iase.disa.mil/stigs/Pages/a-z.aspx
NIST Checklists	https://www.nist.gov/programs-projects/national-checklist-program
NSA Guides	https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/
CIS Benchmarks	https://benchmarks.cisecurity.org/downloads/benchmarks/
SEI CERT Coding Standards	https://www.securecoding.cert.org/confluence/display/seccode/SEI+CERT+Coding+Standards
OWASP Secure Coding Practices	https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide
MS Secure Coding Guidelines	https://msdn.microsoft.com/en-us/library/fkytk30f(v=vs.110).aspx
Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies	https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_Defense_in_Depth_Strategies_S508C.pdf
Vulnerability and Patch Management	
ISO/IEC 30111	https://www.iso.org/standard/53231.html
NIST National Vulnerability Database	https://www.nist.gov/programs-projects/national-vulnerability-database-nvd
CVE Details	https://www.cvedetails.com/index.php
Department of Homeland Security ICS-CERT Division	https://ics-cert.us-cert.gov/advisories
Carnegie Mellon University Software Engineering Institute	https://www.kb.cert.org/vuls/
Guide for Cybersecurity Event Recovery	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

SANS Vulnerability Management	https://www.sans.org/reading-room/whitepapers/projectmanagement/building-vulnerability-management-program-project-management-approach-35932
Customer Security Documentation	
HIMMS/NEMA Manufacturers Disclosure Statement for Medical Device Security (MDS2)	http://www.himss.org/resourcelibrary/MDS2
Software Identification Tags (SWID)	https://nvd.nist.gov/products/swid
Common Platform Enumeration (CPE)	https://csrc.nist.gov/projects/security-content-automation-protocol/specifications/cpe/
Reporting Considerations	
Postmarket Management of Cybersecurity in Medical Devices	https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf
Security Incident Response and Communication	
ISO/IEC 29147	https://www.iso.org/standard/72311.html
Medical Device Cybersecurity Report: Advancing Coordinated Vulnerability Disclosure	http://mdic.org/wp-content/uploads/2018/10/MDIC-CybersecurityReport.pdf
Evaluating Joint Security Plan Progress and Maturity	
Capability Maturity Model Index	http://cmmiinstitute.com/capability-maturity-model-integration
Cyber Threat Source Descriptions	https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions
Overview of Cyber Vulnerabilities	https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities

1058

United States of America	
21 CFR 806	https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=806&showFR=1
HIPAA – HITECH	https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html
National Infrastructure Protection Plan (NIPP)	https://www.dhs.gov/cisa/national-infrastructure-protection-plan

European Union	
93/42/CE	https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993L0042:20071011:en:PDF
EU General Data Protection Regulation (GDPR)	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
Medical Device Regulations (MDR)	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2017:117:TOC
Network and Information Systems (NIS) Directive	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC
Canada	
The Personal Information Protection and Electronic Documents Act (PIPEDA)	https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

1059

1060 **Appendix E: Example Design Input Requirements for** 1061 **Security**

1062 The controls and features included in device design are informed by the device type, design, use
1063 environment, and intended use or functionality. As such, there is no one size fits all set of design
1064 inputs that should be utilized. Design inputs highlighted here in this appendix section are not
1065 intended to be comprehensive; rather, they serve as examples of input requirements that could be
1066 considered within the context of use for a given device. These design input requirements are
1067 categorized by OWASP Security Design Principles.

1068

1069

- **Minimize Attack Surface**

1070

1071

1072

1073

1074

1075

1076

1077

1078

1079

1080

1081

1082

1. The system shall restrict access of removable media to what is necessary for intended use.
2. Execution of software on the system shall be restricted to explicitly authorized or validated software components.
3. The system shall provide capability to anonymize exported data such that an individual or customer is not identifiable.
4. Ports, protocols, services and addresses available on the system and its network connection shall be restricted to the minimum necessary for intended use and configurable locally by authorized user.
5. The system shall be capable of enabling and disabling particular protocol stacks, individual ports and services, and contains manageable host-based firewall.
6. The system shall provide capability to explicitly enable or disable remote access to the system.

- 1083 7. The system shall notify users to change default passwords after initial use.
1084 8. The system shall be capable of restricting repeated and failed user access
1085 attempts.
- 1086 ● **Establish Secure Defaults**
 - 1087 9. The system shall have the ability to require a minimum password length.
 - 1088 10. The system shall have the ability to require a minimum password complexity.
 - 1089 11. The system shall have the ability to require periodic password renewal.
 - 1090 12. The system shall have the ability to restrict password reuse.
 - 1091 13. The system shall have the capability to automatically or manually back-up data
1092 necessary for intended use locally or to an external location.
 - 1093 14. All sensitive information and data shall be encrypted in transit and at rest using an
1094 industry-accepted encryption mechanism and practice.
 - 1095 15. The system shall prominently notify users when sensitive information and data
1096 are displayed on screen or if encryption is disabled in transit.
 - 1097 16. The system shall have routine functionality for handling exceptions, errors and
1098 aborts that does not expose sensitive information and data.
 - 1099 17. The system shall enforce strict order of execution during system start and end.
 - 1100 18. All remote or local user activity which interacts with sensitive information and
1101 data as well as critical functions on the system shall be recorded in an audit log.
 - 1102 19. All audit log entries shall include a start and end date-timestamp, user ID,
1103 role/privileges at time of access, success/failure and a description of the action
1104 performed.
 - 1105 20. The audit log shall locally retain an individual entry for a configurable period of
1106 time or allocation of file system space.
 - 1107 21. The system shall provide capability for a user to reset their own password or
1108 administrative reset, which is logged.
 - 1109 22. The system shall provide the ability to create and assign a unique user ID and
1110 password to each remote or local user.
 - 1111 ● **Principle of Least Privilege**
 - 1112 23. Execution of software on the system shall be limited to the minimum privileges
1113 necessary.
 - 1114 24. The system shall support the creation and assignment of roles that grant the
1115 minimum user privileges necessary for intended use of data and functions.
 - 1116 ● **Principle of Defense in Depth**
 - 1117 25. The system shall support multiple factors for user authentication and capable of
1118 centralized authentication.
 - 1119 26. The system shall provide capability to prevent the execution of known malicious
1120 software.
 - 1121 27. The system shall be capable of manually or automatically locking the display and
1122 requiring user authentication after a configurable period of user inactivity in order
1123 to continue use such that sensitive information and data are not visible.
 - 1124 28. The system shall provide capability for a user to reset their own password or
1125 administrative reset, which is logged.
 - 1126 ● **Fail Securely**
 - 1127 29. The system shall be capable of restoring functionality to an operational state.
1128

- 1129 ● **Don't Trust Services**
- 1130 30. The integrity and composition of all data as input or output of the system shall be
- 1131 validated such that modification is detected and/or rejected.
- 1132 31. All remote or local access to the system by user or an external system shall be
- 1133 authenticated prior to granting access to data or functions.
- 1134 ● **Separation of Duties**
- 1135 32. The audit log shall be restricted in access to only authorized users.
- 1136 33. The audit log shall be exportable and readable by authorized users and have the
- 1137 capability to integrate with security information and event management for real-
- 1138 time analysis.
- 1139 ● **Avoid Security by Obscurity**
- 1140 34. The security of a system shall not rely upon knowledge of the source code or
- 1141 shared hard coded credentials being kept secret.
- 1142 ● **Keep Security Simple**
- 1143 35. The system shall allow security controls to be configured with no significant
- 1144 downtime and centrally managed by authorized users.
- 1145 ● **Fix Security Issues Correctly**
- 1146 36. The system shall support authorized updates to mechanisms for controlling the
- 1147 execution of authorized or malicious software.
- 1148 37. Components of the system shall support software updating and patches with no
- 1149 significant downtime using standard centralized patch management systems.
- 1150

1151 **Appendix F: Example Third-Party Security Agreement**

1152 It is important for vendors to consider the security of various components in their supply chain at
 1153 the time of procurement. This appendix section specifies security requirements applicable to
 1154 third-party suppliers that provide product development and post-market product management
 1155 services to a given vendor.

1156 The supplier is responsible for understanding the risk of [Company] and [Company's]
 1157 customers' information and products it will access, process, manage, or store in the performance
 1158 of services to [Company], and [Company's] customers. Compliance with the Association for the
 1159 Advancement of Medical Instrumentation's (AAMI) "Technical Information Report (TIR) 57 -
 1160 Principles for medical device security—Risk management" is recommended for meeting these
 1161 objectives.

1162 **1. PRODUCT DEVELOPMENT**

- 1163 1.1 Cybersecurity requirements are evaluated and documented during product design.
- 1164 1.2 Cybersecurity threats and risks are evaluated and documented as part of a risk
- 1165 analysis process during product design.
- 1166 1.3 Cybersecurity testing is completed as a part of verification and validation
- 1167 activities. Testing includes, but is not limited to, the following:
- 1168 a) Vulnerability scanning
- 1169 b) Static/binary code scanning
- 1170 c) Fuzz testing
- 1171 d) Customized test cases to evaluate defined cybersecurity
- 1172 requirements

- 1173 e) Penetration tests
1174 1.4 Cybersecurity penetration test is performed before the product is launched.
1175 1.5 Defects identified during security testing shall be documented and evaluated for
1176 correction based on risk analysis process.
1177 1.6 A software inventory or bill of materials shall be documented identifying all
1178 software of unknown provenance (SOUP) and third-party software components in
1179 a device and any backend support and specialist development systems.
1180 a) A security assessment of third party and SOUP components is
1181 performed to determine version and patches are up to date and existing
1182 vulnerabilities are evaluated for risk and corrective action.
1183 b) At the request of [Company] product owners and stakeholders,
1184 documentation and/or evidence of the above shall be made available.
1185 c) At the request of [Company] product owners and stakeholders,
1186 source code and or binary files shall be made available.
1187 d) Licensing arrangements for third party software, that establishes
1188 permissions for use, longevity and liabilities shall be negotiated with
1189 [Company] prior to incorporating such code in code developed for
1190 [Company].
1191 e) Code associated with open source licenses shall be carefully
1192 considered and declared to [Company] and be appraised for the potential
1193 for [Company] to declare or reveal associated intellectual property in the
1194 form of bespoke, contracted code, at any time in the future.
1195

1196 2. POST-MARKET PRODUCT MANAGEMENT

- 1197 2.1 Operating procedures are documented and approved for addressing cybersecurity
1198 patching, updating and remediation.
1199 2.2 A process is defined to facilitate ongoing product change management throughout
1200 the lifecycle of the device.
1201 2.3 A separate testing environment is established for evaluation of patches and
1202 incidents, including necessary devices and connection to backend systems.
1203 2.4 Security measures shall be reviewed including threats, breaches, user access, new
1204 vulnerability reports, assessment of risks and necessary responses, at least
1205 annually or when there is a material change in business practices.
1206 2.5 Training materials and a training plan for administration of the system including
1207 security critical roles and functions shall be established.
1208 2.6 Termination and transfer of people resources from system access, key system
1209 knowledge, and process responsibilities shall be accomplished through
1210 documented processes.
1211 2.7 Product documentation that is publicly available shall be identified and
1212 documented at least annually.
1213 2.8 A process for handling (investigating and remediating) potential vulnerabilities in
1214 products is defined.
1215 2.9 An incident mitigation and response plan is developed, including a timeframe
1216 during which mitigation occurs.

- 1217 2.10 Complaint handling systems include notification to [Company] product owner
1218 and [Company's] product security organization if a cybersecurity complaint is
1219 reported by a customer.
- 1220 2.11 The [Company] product owner and [Company's] product security organization
1221 shall be immediately notified if a cybersecurity issue is identified in a product.
- 1222 2.12 At the request of [Company] product owners and stakeholders, documentation
1223 and/or evidence of the above shall be made available.
1224

1225 **Appendix G: Example Customer Security Documentation**

1226 Customers require security documentation to enable more robust risk assessments, identify
1227 configurable security controls, and allow them to better protect their systems. This appendix
1228 section provides an overview of items that may be included in Customer Security
1229 Documentation. The following are examples of the types of information which may be included
1230 in documentation of security for medical devices or health IT:

- 1231 • Product Description
- 1232 • Hardware Specifications
- 1233 • Operating Systems
- 1234 • Third-party Software
- 1235 • Network Ports and Services
- 1236 • Sensitive Information and Data Transmitted
- 1237 • Sensitive Information and Data Stored
- 1238 • Network and Data Flow Diagram
- 1239 • Malware Protection
- 1240 • Authentication
- 1241 • Network Controls
- 1242 • Physical Controls
- 1243 • Encryption
- 1244 • Audit Logging
- 1245 • Remote Connectivity
- 1246 • Service Handling
- 1247 • End-of-Life and End-of-Support
- 1248 • Secure Coding Standards
- 1249 • System Hardening Standards
- 1250 • Risk Summary
- 1251 • Third Party Certification or Attestation
- 1252 • Manufacturer's Disclosure Statement for Medical Device Security

1253 1254 **Product Description**

1255 [Insert basic description of function or purpose of the product or solution. Photo is optional, but
1256 recommended.]

1257 1258 **Hardware Specifications**

1259 [List hardware components and specs]

1260 • [List]

1261 • [List]

1262 **Operating Systems**

1263 [List hardware operating systems and versions]

1264 • [List]

1265 • [List]

1266 **Third-party Software**

1267 [Also referred to as a Bill of Materials (BOM), includes a list of third-party software and version
1268 numbers where applicable. Having a cybersecurity bill of materials will aid customers in
1269 mitigating cybersecurity concerns on their healthcare technologies and ultimately to the
1270 systems/networks these technologies are attached to. The following are example attributes that
1271 would enable customers to leverage a bill of materials in protecting their assets.

1272 Detailed attributes include:

1273 • All commercial, open source, and custom code must be included

1274 • Commercial technology components (e.g. processors, network cards, sound cards,
1275 graphic cards, memory) must be included

1276 • The software list will be codified using an industry standard, such as Common Platform
1277 Enumeration (CPE), Software Identification tag (SWID), or Software Package Data Exchange
1278 (SPDX) that allows the software list to be searched and used to check against vulnerability feeds

1279 • The list will be available in an electronic format that allows bulk uploading into common
1280 asset inventories, vulnerability management systems and configuration management databases.

1281 • The BOM will be provided to a customer both upon a purchase and after significant
1282 software or hardware upgrades

1283 • Vendors will maintain a BOM for all product versions that will be accessible remotely by
1284 customers]

1285

Vendor and Name	Version	Description
[e.g. Microsoft Windows 10]	[e.g. 1607]	[e.g. Long Term Servicing Branch]

1286 **Network Ports and Services**

1287 [List Network Ports and Services]

Port	Protocol	Service Name	Description of Service	Encrypted	Open/Closed
XXX	XXX	XXXXXX	XXXXXX	XXX	XXX

1288

1289 **Sensitive Information and Data Transmitted**

1290 [List sensitive information and data transmitted. This can include PHI/PII/Potential access to
1291 wireless credentials, etc.]

1292 • [List]

1293 • [List]

1294 **Sensitive Information and Data Stored**

1295 [List sensitive information and data stored. This can include PHI/PII/Potential access to wireless
1296 credentials, etc.]

1297 • [List]

1298 • [List]

1299 **Network and Data Flow Diagram**

1300 [Provide a diagram that describes how the product resides in a customer environment, showing
1301 the system components (1 or N computers, routers, switches, adjacent systems, remote
1302 connectivity) types of connectivity (e.g. RS232, RJ45, Serial to TCP/IP conversion), what types
1303 of data is in transit and at rest (e.g. PHI, QC, config data), and how these are secured (e.g. in
1304 transit IPsec, HTTPS/TLS, WIFI WPA2PSK; at rest BitLocker, SQL TDE)

1305 **Important:** include if the device makes PHI/PII available via network or point-to-point
1306 connection (wired/wireless)?

1307 • Is connected data encrypted in transit?

1308 • Does service have network or p-to-p access to PHI (remote or in-room)?]

1309

1310 **Malware Protection**

1311 [Describe and recommend the anti-malware measures available (e.g. validated AV solutions, AV
1312 partners, how AV is managed, application whitelisting like AppLocker or McAfee Embedded
1313 Control, advanced antimalware solutions, software restriction policies)]

1314

1315 **Patch Management**

1316 [Describe and recommend the method in which we maintain, provide and deploy patch updates
1317 for this product. Examples include, “Patches are installed by a field service engineer during a
1318 routine service visit or during the yearly service visit. In the even that there is no patch
1319 management solution in place, also communicate this in this section.]

1320

1321 **Authentication & Authorization**

1322 [Describe and recommend the controls that customers have with user’s authenticating and
1323 granting permissions to features and functionality, how users are managed, the default use
1324 accounts on the system and how to change and configure accounts. This includes the ability to
1325 disable user accounts]

1326

1327 **Network Controls**

1328 [Describe and recommend the firewall rules, IPSec rules, host file restrictions, browser Internet
1329 access restrictions, MAC and IP address filtering)]

1330

1331 **Encryption**

1332 [Describe and recommend where and how encryption is applied on the system (e.g. all network
1333 traffic is TLS 1.2, at rest is BitLocker with AES 256)]

1334

1335 **Audit Logging**

1336 [Describe the audit logging process, where they are stored, what an auditable event entails, who
1337 has access to audit logs and any file permissions. Describe if audit logs are synchronized with
1338 reliable time sources and have the proper time zone set or no time offset (e.g., GMT or UTC).

1339 • What is the typical and maximum number of records retained on the device when in use?

1340 • Do users have a means to irreversibly delete audit log records in the device?

1341 • Does Service ever retain copies of PHI/PII data (is it encrypted by service) in audit logs?

1342 • Application Auditing

1343 ○ Audit file location: E:\PieRoot\Logfiles*.pld

1344 ○ Audit files hashed with SHA256 when complete for integrity.

1345 ○ Auditable Events:

1346 ■ Service Start/Stop

1347 ■ User login/logout

1348 ■ User session created/destroyed.

1349 ■ User login from multiple workstations.

1350 ■ Client application connect/disconnect with IP address and port.

1351 ■ Failed client connection attempts.

1352 ■ Changes in application configuration.

1353 ■ Failed/successful attempts to access, modify, or delete security objects;
1354 e.g. roles, permissions, etc.

1355 • Audit file permissions:

1356 ○ Administrators group: Read.

1357 ○ Auditors group: Read.

1358 ○ DB Auditors group: Full control.

1359 ○ DB Administrators group: Full control.

1360 ○ Virtual/Managed service accounts (audit file creators): Full control.

1361 ○ Users: None.]

1362 **Remote Connectivity**

1363 [Describe the nature of remote connectivity, what ports, protocols, URLs and endpoints for
1364 communication as well as security measures applied to the remote connection (e.g. TLS)]

1365

1366 **Service Handling**

1367 [Describe what routine maintenance service personnel perform, what security policies and
1368 procedures they follow (e.g. never take PHI or PII, on-site authorization protocol, encrypted
1369 Removable Media, hardened service laptops, whether or not service laptops connect to product,

1370 routine AV update during visit, secure installation/implementation principles, service
1371 authentication to product, decommissioning process, once decommissioned how the product hard
1372 drive is wiped, how the product is recovered from the field or destroyed, and what customer data
1373 and features service personnel interact with)]

1374
1375 **End-of-Life and End-of-Support**

1376 [Describe the life cycle of the product in relation to when it will no longer be sold, updated, and
1377 supported. Provide dates if available otherwise describe how EOL/EOS is communicated.]

1378
1379 **Secure Coding Standards**

1380 [Describe the secure coding standards used]

- 1381 • [List the industry secure coding standards used during software development (e.g. SEI
1382 CERT Java Secure Coding Standard)]

1383 **System Hardening Standards**

1384 [Describe the secure hardening standards used, may also create appendix to list out standards
1385 used.]

Name of Standard	Version Number	Source of Standard
[Insert name of standard]	[Insert version number]	[Insert URL]

1386
1387 **Risk Summary**

1388 [This section should contain a summary of risks found within a penetration test, remediation
1389 report, or other topics and compensating controls that correspond to additional risks outlined in
1390 the product security white paper. This may also include any findings from application scans.]

1391
1392 **Appendix H: Example Organizational Structure**

1393 The intent of this appendix section is to provide an example of roles and responsibilities within
1394 organizations to support the adoption and continuous improvement of cyber security for medical
1395 devices and health IT:

1396
1397 **Medical Device Manufacturers and Health IT Vendors**

- 1398 • **Chief Product Security/Cybersecurity Officer:** Responsibility to drive product and
1399 solution security throughout a vendor organization including identifying best practices
1400 and companywide technical standards, processes, and policies, for overall governance or
1401 guidance. In addition, this individual will advise executive management, product
1402 management, project management, R&D heads and manufacturing heads with regard to
1403 security for all products, solutions and services. Responsible for implementing pre-
1404 market product security design and post-market support including cybersecurity events
1405 and incidents for products in scope. Independent of Information Security and in
1406 cooperation with the CEO, this individual will advise appropriate processes and
1407 structures to introduce security into products, solutions and services.
- 1408 • **Product Security/Cybersecurity Engineering**

- 1409 ○ Security Architects: This person will work with R&D, service, and quality
1410 organizations to research common security vulnerabilities and their remediation;
1411 develop procedures to incorporate hardening into product development; work
1412 with individual product teams in securing their products; and proactively educate
1413 teams across the company on security best practices for products under
1414 development.
- 1415 ○ Penetration Testers: This person will perform security penetration testing, ethical
1416 hacking and red team activities in order to identify unique and common
1417 vulnerabilities in products under development. This includes performing
1418 vulnerability analysis and research, formalizing security testing procedures in the
1419 product lifecycle, performing penetration testing with remediation plans and
1420 formal reporting, and supporting red team, covert, and security activities to test
1421 organizational readiness.
- 1422 ● **Product Security/Cybersecurity Incident Response**
- 1423 ○ Incident Responder: This person will manage technical strategy, process,
1424 timelines, resources and progress for incidents relating to products at customer
1425 sites or with security researchers.
- 1426 ○ Vulnerability Manager: This person will track the escalation, follow-up, and
1427 remediation of vulnerabilities throughout the product lifecycle.
- 1428 ● **Product Security/Cybersecurity Program Management**
- 1429 ○ Policy and Compliance Analyst: This person will ensure the adoption and
1430 continuous improvement of security policies and procedures for products in
1431 compliance with industry standards and regulations.
- 1432 ○ Strategic Program Manager: This person will work cross-functionally to create
1433 programs and initiatives for establishing training, awareness, and fundamental
1434 capabilities for improving security of products.
- 1435 ● **Product Security Testing** – Responsible for assessing and testing products in
1436 development and in the market so as to understand cybersecurity risk and find issues
1437 before an external party does. Comprised of Product Security members and other
1438 participants (such as 3rd parties) as needed.

1439
1440 Larger organizations may choose to have multiple business or product-specific roles
1441 including a dedicated product security officer, manager, and/or engineers.
1442

1443 **Healthcare Provider**

- 1444 ● Healthcare providers may create similar organizational structures to align with vendors
1445 under a Chief Clinical Information Security/Cybersecurity Officer, with distinct
1446 consideration for the healthcare provider’s specific needs relating to security during the
1447 procurement, operation, and decommissioning of medical devices and health IT products.
- 1448 ● A broad set of stakeholders should be involved including people from clinical practices,
1449 medical device support organizations and technology and security areas.

1450

1451 **Appendix I: Example Organizational Training**

1452 The intent of this appendix section is to provide training information that will help organizations
1453 mature their cybersecurity programs. A comprehensive training program for cybersecurity
1454 includes the following:
1455

- 1456 ● **Training Requirements**

1457 Requirements for training each relevant role must be established and periodically
1458 reviewed to determine if they need to be updated.

- 1459 ● **General Awareness Training**

1460 All relevant employees in the organization should understand the principles of
1461 cybersecurity, the framework of the organization's program and the different roles and
1462 responsibilities for cybersecurity.

- 1463 ● **Training by Roles**

- 1464 ○ Training for Security Practitioners

- 1465 ■ Engineers

- 1466 ● Architecture: Security experts who participate in architecting
1467 products or contribute to the security architecture components of
1468 products should be trained in secure architecture principles and
1469 patterns.
- 1470 ● Threat modeling and security risk analysis: Security experts who
1471 participate in threat modeling should be trained in the principles of
1472 threat modeling and the use of threat modeling tools, as well as
1473 methods of translating threats into a risk management framework.
- 1474 ● Design: Security experts who participate in product design or
1475 contribute to the security design of products should be trained in
1476 secure design principles and patterns.
- 1477 ● Testing: Security experts who perform or guide security testing of
1478 products should be trained in security testing methodologies, tools
1479 and interpretation of testing results.
- 1480 ● Forensics and Incident Response: Security experts who evaluate
1481 evidence of security incidents should have training in security
1482 forensic analysis in addition to practical experience. Those who
1483 participate in the incident response process should be trained in
1484 that process and the theory of incident response, in addition to
1485 practical experience.

- 1486 ■ Penetration Testing: Penetration testers should have proper training in
1487 penetration testing techniques and tools as well as considerable practical
1488 experience before being qualified as a penetration tester for products.

- 1489 ■ Security Officers/Directors/Managers/Advocates/Champions: Non-
1490 technical security practitioners should be trained in the secure
1491 development lifecycle, the company's security framework and the
1492 company's quality system.

- 1493 ○ Training for Related Activities – Non-dedicated Practitioners

- 1494 ■ Software/firmware/hardware/systems engineers

- 1495 ● Secure Coding standards: Engineers involved in developing code
- 1496 should be trained in secure coding standards.
- 1497 ● Static and dynamic code analysis tools: Engineers involved in
- 1498 development and/or configuration management should be trained
- 1499 in the use and interpretation of automated code analysis tools.
- 1500 ▪ Sustaining engineering (maintenance for vulnerabilities): Engineers and
- 1501 product managers involved in maintenance of commercialized products
- 1502 should be trained in the interpretation of vulnerability notifications and the
- 1503 steps necessary to respond to vulnerabilities identified in the products.
- 1504 ▪ Risk managers: Risk managers should be trained on the incorporation and
- 1505 interpretation of security risks within the existing risk management
- 1506 framework.
- 1507 ▪ Requirements engineers: Requirements engineers should be trained to be
- 1508 able to incorporate standard security requirements into risk catalogs as
- 1509 well as novel requirements identified during threat modeling.
- 1510 ▪ Deployment engineers: Those responsible for deploying products in the
- 1511 field should be trained on adapting the products to the IT environment as
- 1512 well as configuring that environment, to match the security requirements
- 1513 specified for the products.
- 1514 ▪ Support and service engineers: Support and service engineers should be
- 1515 trained to recognize, remediate and escalate security issues reported or
- 1516 discovered in fielded systems.
- 1517 ▪ Information Security/IT/Systems Administration (infrastructure): Those
- 1518 responsible for defining and implementing the security infrastructure of
- 1519 the company's IT and physical environments should be trained in the
- 1520 access and protection requirements of secure development and
- 1521 manufacturing.
- 1522 ● **Periodic refreshers for awareness:** Employees who have participated in the overall
- 1523 awareness and more detailed training should be given periodic refresher training to
- 1524 remind them of the key elements of the previously acquired training.
- 1525 ● **Periodic updates for changes in threat landscape, technology, program:** As the threat
- 1526 landscape changes, as new technology is developed in cybersecurity and as the
- 1527 company's security program evolves, the training requirements and trainings themselves
- 1528 should be updated to stay in synchronization.
- 1529 ● **Qualification and Certification of Security Experts:**
- 1530 ○ Certification: Requirements for certification for security experts and practitioners
- 1531 should be established and upheld as minimum qualifications to participate in these
- 1532 activities. Certifications can be external and/or internal (based on completion and
- 1533 confirmation of an internal training regime).
- 1534 ○ On the job experience: Minimum requirements for actual experience practicing
- 1535 security activities should be specified for a person to be considered a security
- 1536 expert in a particular sub-role of expertise.
- 1537 ○ Mentoring and community: Participation in the community of experts within the
- 1538 company should be included as a requirement to be considered a security expert.
- 1539 This may include peer relationships as well as mentor-mentee relationships.

- 1540 ○ Levels of expertise: Different levels of expertise should be defined by the degree
1541 to which a practitioner has achieved these aspects of qualification. The levels
1542 should correspond to minimum requirements for specific security-related
1543 activities. For instance, a penetration tester may be allowed to be the lead tester
1544 for a product only in the case of a minimum amount of time practicing as a
1545 penetration tester.
- 1546 ● **Drills:** Periodic drills should be exercised, in order to ensure the ability of practitioners to
1547 apply trainings. These may take the form of tabletop incident response drills or full-
1548 blown red team/blue team exercises.

1549

1550 **Appendix J: Example Security Risk Assessment Methods**

1551 **Common Vulnerability Scoring System Rubric for Healthcare**

1552 CVSS provides a way to characterize and assess the severity of a cybersecurity vulnerability, and
1553 the IT industry has used it effectively to manage system and software vulnerabilities for many
1554 years. The purpose of this appendix section is to provide additional healthcare context for end
1555 users and vendors that leverage CVSS as a part of their vulnerability assessment.

1556 CVSS and its associated rubric and examples were developed for enterprise information
1557 technology systems and do not adequately reflect the clinical environment and potential patient
1558 safety impacts. As such, a CVSS supplemental rubric tailored to explicitly consider the clinical
1559 environment and potential impacts to patient safety is being developed in collaboration with
1560 subject matter experts across the medical device ecosystem. The intent is to use the rubric with
1561 CVSS to provide a consistent and standardized way to communicate the severity of a
1562 vulnerability between multiple parties, including the medical device manufacturer, hospitals,
1563 clinicians, patients, Department of Homeland Security (DHS), and vulnerability researchers.

1564 The draft “Rubric for Applying CVSS to Medical Devices” is found at
1565 <https://www.mitre.org/md-cvss-rubric>.

1566

1567 **Appendix K: CMMI® for Development**

1568 CMMI for development is a reference model that includes activities and best practices for
1569 developing products and services. There are 5 CMMI maturity levels from level 1 to level 5 and
1570 these maturity levels provide a means for organizations to assess and describe their performance.
1571 This appendix section provides an overview of these maturity levels which may also be found at
1572 <https://cmmiinstitute.com/learning/appraisals/levels>.

1573

1574 **Maturity Level 1: Initial**

1575 At maturity level 1, processes are usually ad hoc and chaotic. The organization usually does not
1576 provide a stable environment to support processes. Success in these organizations depends on the
1577 competence and heroics of the people in the organization and not on the use of proven processes.
1578 In spite of this chaos, maturity level 1 organizations often produce products and services that
1579 work, but they frequently exceed the budget and schedule documented in their plans. Maturity
1580 level 1 organizations are characterized by a tendency to overcommit, abandon their processes in

1581 a time of crisis, and be unable to repeat their successes.

1582

1583 **Maturity Level 2: Managed**

1584 At maturity level 2, the projects have ensured that processes are planned and executed in
1585 accordance with policy; the projects employ skilled people who have adequate resources to
1586 produce controlled outputs; involve relevant stakeholders; are monitored, controlled, and
1587 reviewed; and are evaluated for adherence to their process descriptions. The process discipline
1588 reflected by maturity level 2 helps to ensure that existing practices are retained during times of
1589 stress. When these practices are in place, projects are performed and managed according to their
1590 documented plans.

1591 Also at maturity level 2, the status of the work products are visible to management at defined
1592 points (e.g., at major milestones, at the completion of major tasks). Commitments are established
1593 among relevant stakeholders and are revised as needed. Work products are appropriately
1594 controlled. The work products and services satisfy their specified process descriptions, standards,
1595 and procedures.

1596

1597 **Maturity Level 3: Defined**

1598 At maturity level 3, processes are well characterized and understood, and are described in
1599 standards, procedures, tools, and methods. The organization's set of standard processes, which is
1600 the basis for maturity level 3, is established and improved over time. These standard processes
1601 are used to establish consistency across the organization. Projects establish their defined
1602 processes by tailoring the organization's set of standard processes according to tailoring
1603 guidelines. (See the definition of "organization's set of standard processes" in the glossary.)

1604

1605 A critical distinction between maturity levels 2 and 3 is the scope of standards, process
1606 descriptions, and procedures. At maturity level 2, the standards, process descriptions, and
1607 procedures can be quite different in each specific instance of the process (e.g., on a particular
1608 project). At maturity level 3, the standards, process descriptions, and procedures for a project are
1609 tailored from the organization's set of standard processes to suit a particular project or
1610 organizational unit and therefore are more consistent except for the differences allowed by the
1611 tailoring guidelines.

1612

1613 Another critical distinction is that at maturity level 3, processes are typically described more
1614 rigorously than at maturity level 2. A defined process clearly states the purpose, inputs, entry
1615 criteria, activities, roles, measures, verification steps, outputs, and exit criteria. At maturity level
1616 3, processes are managed more proactively using an understanding of the interrelationships of
1617 process activities and detailed measures of the process, its work products, and its services.

1618 At maturity level 3, the organization further improves its processes that are related to the
1619 maturity level 2 process areas. Generic practices associated with generic goal 3 that were not
1620 addressed at maturity level 2 are applied to achieve maturity level 3.

1621

1622 **Maturity Level 4: Quantitatively Managed**

1623 At maturity level 4, the organization and projects establish quantitative objectives for quality and
1624 process performance and use them as criteria in managing projects. Quantitative objectives are
1625 based on the needs of the customer, end users, organization, and process implementers. Quality

1626 and process performance is understood in statistical terms and is managed throughout the life of
1627 projects.

1628
1629 For selected subprocesses, specific measures of process performance are collected and
1630 statistically analyzed. When selecting subprocesses for analyses, it is critical to understand the
1631 relationships between different subprocesses and their impact on achieving the objectives for
1632 quality and process performance. Such an approach helps to ensure that subprocess monitoring
1633 using statistical and other quantitative techniques is applied to where it has the most overall
1634 value to the business. Process performance baselines and models can be used to help set quality
1635 and process performance objectives that help achieve business objectives.

1636
1637 A critical distinction between maturity levels 3 and 4 is the predictability of process
1638 performance. At maturity level 4, the performance of projects and selected subprocesses is
1639 controlled using statistical and other quantitative techniques, and predictions are based, in part,
1640 on a statistical analysis of fine-grained process data.

1641 **Maturity Level 5: Optimizing**

1642 At maturity level 5, an organization continually improves its processes based on a quantitative
1643 understanding of its business objectives and performance needs. The organization uses a
1644 quantitative approach to understand the variation inherent in the process and the causes of
1645 process outcomes.

1646
1647 Maturity level 5 focuses on continually improving process performance through incremental and
1648 innovative process and technological improvements. The organization's quality and process
1649 performance objectives are established, continually revised to reflect changing business
1650 objectives and organizational performance, and used as criteria in managing process
1651 improvement. The effects of deployed process improvements are measured using statistical and
1652 other quantitative techniques and compared to quality and process performance objectives. The
1653 project's defined processes, the organization's set of standard processes, and supporting
1654 technology are targets of measurable improvement activities.

1655
1656 A critical distinction between maturity levels 4 and 5 is the focus on managing and improving
1657 organizational performance. At maturity level 4, the organization and projects focus on
1658 understanding and controlling performance at the subprocess level and using the results to
1659 manage projects. At maturity level 5, the organization is concerned with overall organizational
1660 performance using data collected from multiple projects. Analysis of the data identifies shortfalls
1661 or gaps in performance. These gaps are used to drive organizational process improvement that
1662 generates measurable improvement in performance.

1664

1665 ##