7

Security Risk Management

Ben Kokx

Introduction

Information Technology (IT) systems are becoming increasingly essential in all facets of work and daily life, from mobile phones to desktop and laptop computers to the servers and infrastructure that support them. In healthcare, this includes hospital back-office IT systems; building automation such as Heating, Ventilation, and Air Conditioning Systems (HVAC) and door locks; and medical IT (medical devices, in-vitro diagnostics [IVDs], Software as Medical Device [SaMD], health IT systems, and workstations).

As healthcare becomes increasingly digitalized, the number of IT systems used to provide care is also rapidly increasing. As more health IT systems are introduced, their functionality has also been extended, which often requires them to be connected to other systems and even via the internet. This need for connectivity brings significant advantages but also great risks, as these systems can be more easily influenced by the IT environment and by people who either accidentally or with malicious intent disrupt or block access to the IT systems or delete, modify, and copy data from the system for financial gain or other motives.

Product safety and performance of software-supported medical devices and IVDs may be affected by security, as acknowledged in the third edition of ISO 14971.[1] Some regulations focus on safety and performance without explicitly calling out security, or they only provide high-level security requirements. An increasing number of healthcare-related regulatory guidance documents have provided more detail on how regulators expect manufacturers to address these security concerns. Recent regulatory changes in the US, for example, are requiring manufacturers to ensure the cybersecurity of their medical devices, extending beyond the impact on safety and essential performance.[2]

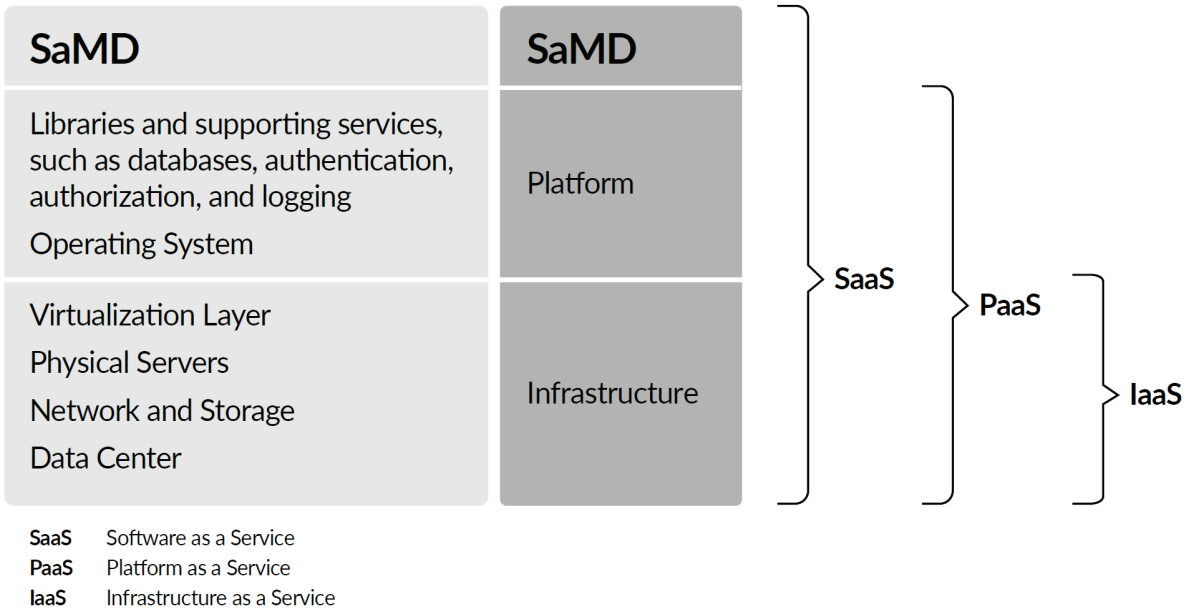
Many healthcare-related regulatory guidance documents use the words security or cybersecurity. Technically, cybersecurity can be considered a subset of security. Cybersecurity deals with protecting data and information in digital or electronic form, while security also involves safeguarding physical assets. Although they have different meanings, the words are often used interchangeably. The word security is used throughout this chapter without the intention of distinguishing between the terms. SaMD also requires security measures in the physical world to protect assets, for instance, by placing the network server that runs the software in a locked cabinet within an access-controlled room in a physically secured building.

The increase in ransomware attacks worldwide affects hospitals' ability to provide care due to the unavailability of both clinical and non-clinical systems, including electronic patient records. Although there is no evidence that the WannaCry attack on the National Health Service (NHS) in the UK in 2017 led to a higher mortality, it was disruptive, with a substantial financial impact.[3] A cyberattack contributed to the death of a person in Düsseldorf, Germany, in September 2020, by delaying patient treatment because the emergency department of the nearby hospital was closed due to a cyberattack. The patient died shortly after arriving at another hospital an hour later. After a two-month investigation, the public prosecutor in Cologne concluded that there were insufficient grounds to pursue the hackers for negligent homicide. Although ransomware was involved in the case, there were no means to establish legal causation to determine whether the hackers, if they could be identified, contributed sufficiently to the fatality.[4] The first death that was linked to a ransomware attack was confirmed by the NHS in the UK, where an attack caused a long delay in blood-test results, which contributed to the patient's death.[5] With the increase in ransomware attacks targeting the healthcare sector, manufacturers and hospitals can expect more negative outcomes and need to implement adequate security measures to reduce such risks.[6,7]

SaMD Security

Security risk management should always consider both the platform on which the software runs and the infrastructure in which the software and platform operate (see **Figure 7-1**). As

Figure 7-1. SaMD Security



Created by Ben Kokx

such, dealing with security risk management for SaMD is no different than for any other software, such as embedded software and Programmable Electrical Medical Systems (PEMS).

Manufacturers should conduct security testing, such as fuzz testing, vulnerability scanning, and penetration testing, on systems configured in accordance with their intended operational use environment. This testing verifies and validates not only the software but also the technical and/or organizational measures defined for the intended operational use environment. For completeness, such tests also should be conducted by the manufacturer in a test environment with administrative credentials or the security controls on the platform and the infrastructure disabled, to understand the SaMD impact and risks when security controls fail in each layer of defense. The product should support the ability for the healthcare provider to perform security testing as required by internal policy and legal obligations.

A manufacturer needs to recognize that they might have limited control over the platform and infrastructure on which the SaMD operates. For instance, the SaMD might be running on a system shared with other software applications and other users. Furthermore, there are no warranties that the SaMD and supporting platform and software are kept up to date by the user, resulting in multiple versions and combinations being used on the market.

One of the key differences in SaMD security compared with embedded software and PEMS is the varying level of responsibility for specific activities, which depends on how the SaMD is deployed and managed. Is it sold as a software-only product, an on-premises solution, an off-premises solution (cloud), or a hybrid solution? For each deployment option, specific operational responsibilities shift from the manufacturer to the customer/user. In most scenarios, the manufacturer and/or the user might involve third parties to perform parts of the operational responsibilities.

Therefore, there is a need to establish and document the security responsibility boundaries, to ensure that responsibilities for establishing and maintaining the technical and/or organizational measures provided by the SaMD, the platform, and the infrastructure are clearly defined and documented for the manufacturer, the user, and any integrators or service organizations under the user's or manufacturer's authority. The following are some examples of such responsibilities:

- Who provides the platform, supporting software, and infrastructure that the SaMD operates on–for instance, the server with operating system and supporting software components, such as databases, authentication services, central logging services, and endpoint protection software?
- Who will install and configure all the software, including the platform and supporting software?
- Who is responsible for the maintenance, such as installing updates, of the SaMD?
- Who is responsible for the daily operation and maintenance of the platform, supporting software, and infrastructure?
- Will the manufacturer validate the patches of the platform and supporting software components before the user can install them, or is this entirely the user's responsibility?
- If the manufacturer validates the patches, how will this be communicated, and how often?
- If the user maintains the platform, is there a need to validate that the software is still functioning as intended

after patching or after configuration changes to the operating system, supporting software, and/or infrastructure? If yes, how can the user validate that the software is still functioning as intended?
- Next to maintenance/patches, who will be responsible for validating the operating system and supporting software upgrades to ensure compatibility with newer versions?
- Is there a need for data backups, redundant systems, and so on? If so, who is responsible?

Manufacturers should identify the technical and/or organizational dependencies and measures, supported by a security risk assessment, and clearly document these. Manufacturers should clearly identify in customer-facing documentation which security features their product provides and which security controls the deployer needs to implement to establish a shared security responsibility between the operator and the manufacturer. That information should be part of user-facing documentation and is often also explicitly required from a regulatory perspective, such as in the EU through the general safety and performance requirements in the EU MDR[8] Annex 1, articles 17.4 and 23.4 (ab), and in the EU IVDR[9] Annex 1, articles 16.4 and 20.4 (ah), and further expressed in detail in the Medical Device Coordinators Group 2019–16 guidance on cybersecurity for medical devices[10] (Chapter 3.6, Minimum IT requirements).

Security Risk Management

Manufacturers must perform security risk management, which involves the following aspects related to a SaMD:
- Software development
- Software manufacturing (build and release)
- Management of the software/service (including software installation and updates)
- Management of the platform (operating system and supporting software)
- Management of the infrastructure (network and data centers)

ISO 14971:2019 deals with risk management for medical devices, including software as a medical device and in vitro diagnostic medical devices. In this standard, the term safety is defined as freedom from unacceptable risk (ISO 14971:2019, 3.26), and this risk is not restricted to any specific risk areas. Therefore, safety encompasses freedom from unacceptable risks related to security, or more specifically, freedom from unacceptable risks arising from security breaches. All risks are related to possible harm, which is defined broadly in ISO 14971:2019, 3.3. The broad concept of risk, explicitly including security risks, is explained several times and is stated in Annex A as follows:

The process described in ISO 14971 can be applied to hazards and risks associated with the medical device. Risks related to data and systems security are specifically mentioned in the scope, to avoid any misunderstanding that a separate process would be needed to manage security risks related to medical devices. This does not preclude the possibility of developing specific standards, in which specific methods and requirements are provided for the assessment and control of security risks.

The International Medical Device Regulators Forum (IMDRF) document, Software as a medical device: Possible framework for risk categorization and corresponding considerations,[11] defines several considerations for manufacturers in Chapter 9.3 when identifying implications for the safety and performance of SaMD. The document points out that there can be vulnerabilities in software components, but also design flaws in access controls and infrastructure, unprotected interfaces, and ways to bypass security controls (backdoors). Security must not only address safety and performance, but also data protection and issues that could be exploited as a stepping stone to attack other systems within the user's infrastructure. Risk assessment should focus on the system view, which expands beyond the SaMD to understand risks from and to other connected devices. Threat modeling can help identify these weaknesses.

Security by Design

Security risk management is addressed through the security-by-design process activities, also known as a secure software development framework. These activities typically have the following elements:
- Product security plan document(s) should be created, in which the cybersecurity management activities that must be executed during the total product lifecycle are described. This plan ensures that budget and resources are allocated to continuous efforts, such as monitoring, testing, and vulnerability handling, and that product updates, upgrades, and end-of-life planning are in place.
- Elicit requirements to assess which security requirements must be implemented to satisfy the manufacturer and end-user regulatory requirements, contractual obligations, and any security risks that are identified.
- Security risk assessments must be conducted at every development stage, from very early stages to the end of support. Security risk assessment is based on the output of threat modeling and takes further input from various sources, including documents created through continuous security testing. Traceability to the safety risk management is key. The AAMI SW96 Standard for Medical Device Security–Security Risk Management for Device Manufacturers[12] can provide further guidance.
- Secure design ensures that products are secure on every interface, applying least privileged and defense-in-depth approaches, utilizing secure components and design patterns, and so on.
- Secure implementation practices include secure coding, validating all inputs, correct error handling, static and dynamic code analysis, and a review of the security implementation and its traceability to the design requirements.
- Verification and validation that the product meets the security requirements with the agreed-upon level of

assurance, and conduct appropriate testing, such as but not limited to vulnerability scanning, fuzz testing, penetration testing, resource attacks, and security rule violations.
- Documentation of the security capabilities and security requirements for the intended use environment to support the users in the correct, secure use and their security risk assessments.
- Security monitoring to ensure that security issues that might impact safety, effectiveness, or data and system security are discovered and addressed without undue delay during the total product lifecycle. Security monitoring includes, but is not limited to, newly discovered vulnerabilities, security incidents that occurred in the field, end-of-support declarations for components, continuous testing reports, coordinated vulnerability disclosure and other relevant documents.
- Security issue management is the treatment of any security issues without undue delay to determine mitigating actions (e.g., updates, upgrades, recalls) and the necessity of customer/regulatory reporting obligations.

IEC 81001-5-1:2021 Safety, security and effectiveness in the implementation and use of connected medical devices or connected health software–Part 5: Security–Sub-Part 5-1: Security - Activities in the product lifecycle is a healthcare-specific process standard that extends the IEC 62304 with the activities for security risk management.[13] This standard is recommended for the US and Europe, and is a regulatory requirement for Japan. An alternative standard recognized by the US Food and Drug Administration (FDA) is NIST SP 800-218.[14]

The FDA guidance for Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions provides further guidance on the expectations manufacturers have regarding security risk management.[15] The FDA eSTAR form for 510(k) submissions contains detailed information on the documentation and evidence that manufacturers need to provide.[16]

Threat Modeling

Threat modeling is a systematic approach for analyzing an item's security in a structured way, such that weaknesses can be identified and prioritized. Manufacturers can apply threat modeling to a wide range of items, including software, devices, systems, networks, distributed systems, and business processes. Threat modeling typically identifies attack vectors and assets most desired by an attacker. It requires a decomposition of the items (software, device, system, etc.) to examine each possible attack vector for each item individually, and to determine the type of attacks for which they are vulnerable. The created list of vulnerabilities can be ordered in terms of risk, potential to impact safety, effectiveness, or any other criteria deemed appropriate, such as privacy. Various threat modeling techniques are available, ranging from making a simple list of known vulnerabilities, common attack methods, and common programming mistakes for the components and design, such as the Open Web Application Security Project,[17] Common Attack Pattern Enumeration and Classification,[18] and Common Weakness Enumeration,[19] or specific threat modeling frameworks can be adopted, such as DREAD, OCTAVE, STRIDE, TRIKE, and VAST. Annex A of the white paper, IEEE Personal Health Devices Cybersecurity Standards Roadmap,[20] provides an overview of several frameworks and methodologies.

Threat modeling typically includes the development of detailed architecture diagrams and data flow diagrams, including data classification. A threat modeling playbook, developed by MITRE with support from the FDA, provides a thorough introduction.[21]

If a new vulnerability adds to a specific attack vector, compromises a previously unseen use case, or introduces a new risk that has not been previously assessed in the safety risk assessment, then an update of the safety risk assessment is also necessary. However, many security vulnerabilities have the same attack vectors and impact. Instead of documenting dozens of almost similar security issues, one could choose to combine these vulnerabilities into specific groups or classes with a common impact on safety, confidentiality, integrity, and availability, as in the following:
- Network access vulnerabilities:
  - Resulting in root access without authentication
  - Resulting in root access for any authenticated user
- Elevation of privilege:
  - To root for any authenticated interactive local users
  - To obtain unauthorized access to patient data
- Draining systems resources:
  - Central Processing Unit (CPU)
  - Memory

The IMDRF document, Principles and Practices for Medical Device Cybersecurity, provides additional guidance.[22]

Vulnerability Handling and Security Monitoring

SaMD relies on third-party software components, on which functionality might even be provided by services running on other systems and even other infrastructures. In the 2019 update of the off-the-shelf software (OTS) guidance, the FDA acknowledges that the use of OTS software has expanded in tandem with the widespread adoption of general-purpose computer hardware.[23] In the introduction, the FDA states the following: "The medical device manufacturer using OTS Software generally gives up software lifecycle control, but still bears the responsibility for the continued safe and effective performance of the medical device."

From a security perspective, there is a need to understand the contents of any third-party software in more detail; for instance, an imaging library may combine several other open-source software packages, each of which might have specific security vulnerabilities. In this respect, the detail of software decomposition required for adequate security analysis may extend beyond what is typically provided in a list of software

of unknown provenance. Third parties typically provide these details in a software bill of materials (SBOM). Tools that can analyze an SBOM and compare it with vulnerability databases are required to be able to do proper vulnerability handling. The IMDRF document Principles and practices for software bill of materials for medical device cybersecurity provides further insights.[24]

All software is prone to vulnerabilities that could, for example, be introduced by poor design, inadequate coding practices, improper fault handling, or compiler-introduced security issues, or which may even be inherent in hardware, such as CPUs. Attackers may find vulnerabilities in the manufacturer's software as well as in any third-party software and hardware used. The more commonly used the software is, the more attractive it is to attackers, and therefore, it presents a greater possibility that new vulnerabilities will be discovered.

A vulnerability does not in itself directly introduce a risk. Only when the vulnerability can be exploited by a person or by malicious software attacking the underlying system or infrastructure, does it become a risk. Some vulnerabilities remain undiscovered for many years; for instance, CVE-2020-1317, a serious vulnerability in the Windows Group Policies, lingered in the Microsoft Windows operating system since 2008 before it was discovered and publicly disclosed on 9 June 2020.[25] Once discovered, the probability that a vulnerability will be exploited may remain low if the attack is complex, especially if multiple vulnerabilities must be exploited for a successful attack. However, when a successful attack has been published and proof-of-concept code has been made available, the probability increases significantly, as the attacker's required skill level is reduced to perform a successful attack.

Threat actors capable of complex attacks aim to prevent the discovery of their attacks and the vulnerabilities they exploit, thereby hiding their malicious activities for as long as possible. For the same reason, they might target less commonly used software or even target specific software from a single vendor.

As thousands of security vulnerabilities are discovered and reported every month, it is crucial to be aware of new vulnerabilities promptly. Security monitoring should start while a SaMD is still in development to remediate any vulnerabilities as early as possible; this monitoring should continue throughout the SaMD's total product lifecycle. Security monitoring should also begin during the design phase and continue during the operation of the SaMD's intended operational use environment (platform and infrastructure), under the control of the manufacturer or user.

Security vulnerability analysis should be triggered at specific intervals, such as weekly or monthly, based on factors including the type of SaMD, its components, the supporting platform and network infrastructure used, and the associated risks. An analysis should also be triggered and expedited by specific events or security issues the manufacturer becomes aware of. These indicators might originate from sources such as:

- Complaints and security incidents;
- Vulnerabilities and patches reported by suppliers of components;
- Security issues reported by tool vendors (e.g., compilers and software development kits);
- New risks identified by other third parties (a coordinated vulnerability disclosure, media outlets, the security community, an information sharing and analysis center [ISAC], a computer emergency response team [CERT], national cyber security center, etc.);
- Vulnerabilities identified by running security test tools (e.g., vulnerability scanning, pen testing, fuzz testing, secure code analysis, and software bill of material analysis tools);
- Attacks on the infrastructure;
- New risks identified in internal components and similar products; and
- Changes in the threat landscape.

Security monitoring is a continuous process. **Figure 7-2** shows an exemplary generic monitoring flow.

Although the SaMD manufacturer sets the requirements for the intended operational use environment (platform, supporting software, and infrastructure) on which the SaMD runs, security monitoring can be the responsibility of multiple organizations (hereafter referred to as the responsible organization).

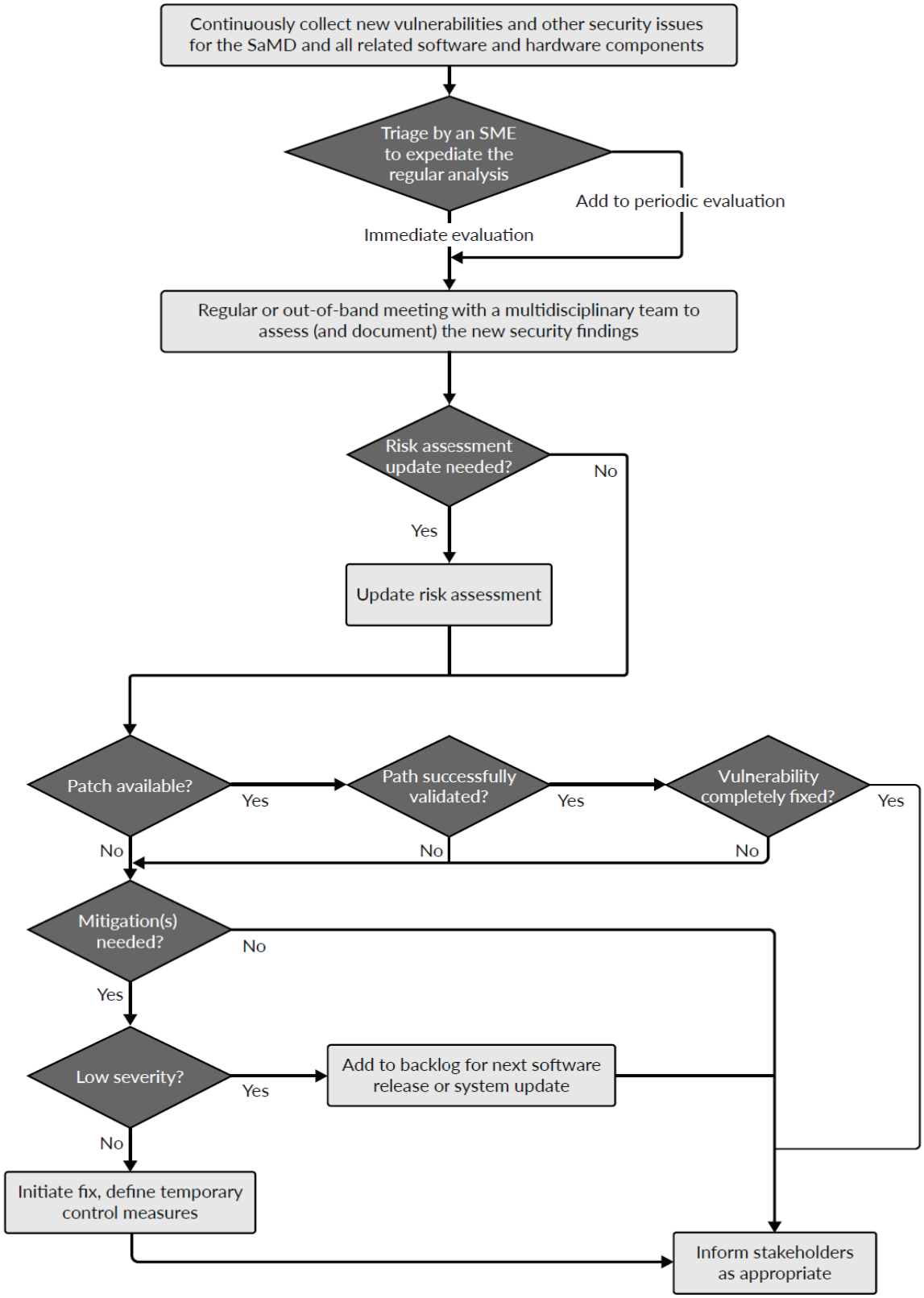
We often become aware of a new vulnerability when the original component manufacturer releases a patch; if a patch is available to mitigate this latest vulnerability, it needs to be validated to ensure it does not cause a conflict with the SaMD or its platform, supporting software, or infrastructure. The manufacturer must perform this assessment to ensure that safety and performance are not impacted. On the other hand, installing patches could lead to other failures that impact system functionality or performance, break security controls, or cause interoperability issues.

Even if the maintenance of the platform, supporting software, and infrastructure is the user's responsibility, the manufacturer should also perform security monitoring against the defined intended operating use environment. Informing the SaMD users of incompatible patches with the defined platform and infrastructure is crucial.

Suppose a patch is unavailable or is incompatible with the SaMD or the platform. In that case, the manufacturer may need to introduce additional mitigations to ensure the vulnerability resolved by the patch cannot be exploited. This consideration also should be made if the patch does not mitigate all discovered security issues. Mitigations could include design changes or additional security controls, such as temporarily limiting network access to specific IP addresses or network ports, completely isolating the system from the network, or implementing specific configuration changes, like denying access to external users. Note that these mitigations might impede certain functionality.

When design changes or mitigating controls are needed, they can be made available on short notice for implementation by the responsible organization. Alternatively, if changes are considered low-risk, they can be implemented at the next scheduled maintenance window. In any case, the manufacturer should determine who needs to be provided with

Figure 7-2. Security Monitoring Flowchart



Created by Ben Kokx

what information for appropriate actions and the transfer of responsibilities.

As stated above, the actual implementation might differ, depending on how the manufacturer deploys the SaMD. For example, suppose an SaMD is an SaaS solution operated by the manufacturer. In that case, it may not be necessary to inform the user about every patch that is installed on the cloud infrastructure. In contrast, if the user needs to patch the on-premise or hybrid SaMD, it may be necessary to inform the user of validated and/or conflicting patches or about temporary mitigations that stakeholders should be taking into consideration until a permanent solution is available.

Informing stakeholders also includes reporting security risks, as required by various laws and regulations, contractual obligations, or other specific needs, such as informing a supplier or open-source community of issues discovered in their software component, or providing input to an ISAC or CERT for sharing information with the healthcare community.

The FDA postmarket guidance provides further guidance on monitoring and vulnerability handling.[26]

Total Product Lifecycle

It is not sufficient to monitor only for security vulnerabilities to manage security during the entire SaMD lifecycle. Changes in the threat landscape can also occur, such as new methods of attacking systems and infrastructures, broken protocols, or compromised cryptography. Ransomware attacks have been one of the biggest changes in the hospital's threat landscape in recent years.

Furthermore, software may become obsolete if the original manufacturer or the open-source community no longer supports a component or a specific version. Therefore, to avoid obsolescence issues, the SaMD manufacturer should promptly validate patches, version upgrades, and replacements of any software components, the operating system, and supporting software. Mitigation measures should include any security risks that cannot be mitigated by patches or incompatibility issues that impact safety and performance. Furthermore, patches, updates, and upgrades can cause an increased security risk because specific security measures designed into the SaMD, platform, or infrastructure are no longer effective.

When the security of a SaMD can no longer be guaranteed, the manufacturer should declare the SaMD as legacy, as explained in the IMDRF guide on Principles and practices for the cybersecurity of legacy medical devices.[27]

As stated earlier, the manufacturer should be aware and consider security evaluations for multiple versions and combinations potentially in use on the market. An active approach to limit the number of supported versions in the field could reduce the amount of effort required.

Shared Responsibility

Managing security involves a combination of technical and organizational measures implemented by all parties involved at the various levels, including components, systems, and network infrastructure. As such, there is rarely a single organization entirely responsible for everything, from the manufacturer developing the SaMD to the clinical user using a hospital-managed workstation to access or run the software.

A SaMD can be developed securely by the manufacturer. Still, if the user is responsible for the platform on which the software runs, and that platform does not receive the necessary operating system and application hardening, such as access controls and endpoint protection software, the probability of a successful attack increases. If the network infrastructure is not secure and the SaMD is unintentionally exposed to the internet while the manufacturer did not design it for that purpose, there is yet again an increased probability of an attack. The healthcare delivery organization and manufacturing staff need to understand how to address security risks, such as malicious emails that could compromise the network or software running on it. Both organizations have specific roles for ensuring secure operations.

Risk transfer is not the intended outcome of shared responsibility. A manufacturer cannot claim that the SaMD's security is not their responsibility, as the user needs to ensure a secure network. The manufacturer, the healthcare delivery organization, and any other third party involved must play their respective roles in the defense-in-depth strategy. The SaMD must be secure in itself; the operating system and support software must be secure independently; the network infrastructure must be secure; and the staff must be made aware of security risks and maintain good security hygiene. A defense is effective only if security is adequately established at all layers and implemented by all stakeholders. ISO 81001-1 provides the principles and concepts for healthcare, including the roles and responsibilities of all stakeholders.[28]

Every organization in the supply chain must conduct due diligence to ensure that it only uses and integrates secure systems, services, and components. This due diligence applies to the healthcare delivery organization, as well as to its suppliers and the suppliers of those suppliers. At any stage in the supply chain, security vulnerabilities can be introduced intentionally, unintentionally, or even maliciously.

To support shared responsibility and address supply chain security, manufacturers should be transparent about the security capabilities of their products and services. These capabilities need to be documented in the instructions for use, administrative guides, security white papers, and other deliverables. The Manufacturer disclosure statement for Medical Device Security (MDS2) is regarded as an important tool to provide security-relevant information to the healthcare delivery organization.[29] The use of the MDS2 is also supported by regulatory guidances and healthcare procurement guides.

Standards

Many standards address security. The selection depends on the intended use, intended operational use environment, deployment choices, such as software-only product, on-premise solution, off-premise solution (cloud), market access

requirements, technology choices, and applicable regulations for the manufacturer and user.

Addressing security can be complex when the manufacturer uses different standards to demonstrate compliance with the requirements of specific laws and regulations. The following are some examples of commonly used security standards:

- Operational security for the manufacturer, healthcare delivery organization, and any third-party IaaS/PaaS providers:
  - ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 27799
  - NIST Cybersecurity Framework, NIST SP 800-53
  - ISO/IEC 27034 series
  - IEC 80001-1
  - ISO 81001-1
- Cloud service providers and users:
  - ISO/IEC 27017
  - ISO/IEC 27018
  - ISO/IEC 27701
- Security requirements for manufacturer processes:
  - IEC 81001-5-1
  - NIST SP 800-218 (SSDF)
  - IEC 62443-4-1
- Security requirements for the SaMD product:
  - IEC/TR 60601-4-5
  - IEC/TS 81001-2-2
  - IEC 62443-4-2

Overlapping Legislative Security Requirements

The confidentiality, availability, and integrity of systems and data not only can impact safety and performance, but also the mission of the healthcare delivery organization at large, including its ability to comply with other legislative obligations, such as data protection legislation like the General Data Protection Regulation (EU) 2016/679 in Europe and the Health Insurance Portability and Accountability Act (HIPAA) in the US.

Across the globe, policymakers and regulators are introducing security requirements in a variety of new laws and regulations to protect society at large by strengthening the cyber resilience of the healthcare sector and other critical infrastructures against the increasing cybersecurity threats. Geopolitical changes are extending cyber threats from criminals for financial gain to include state actors for cyber-warfare.

The update of the Network Information Security Directive (NIS2; (EU) 2022/2555) in Europe sets reporting requirements for the critical infrastructure, but now also addresses the supply chain. NIS2 also directly applies to healthcare delivery organizations, managed service and cloud providers, and medical device manufacturers in Europe. As a directive, additional requirements at the national level from the national NIS2 implementation might impact the features and configuration of the SaMD, the operating system, and supporting software, as well as the infrastructure. For instance, specific requirements for strong encryption on the network for sensitive data, such as electronic patient records or national identifiers, might break communication with systems on the network that do not support the required cryptographic methods.

When addressing additional legislative requirements, consideration must always be given to safety and effectiveness. For instance, requiring multi-factor authentication before being able to view patient information on a vital life signs monitor might protect personal data from a privacy legislative perspective, but also raises a patient safety concern, as necessary information might not be directly available in case of an emergency, which could delay treatment and thus could impact patient safety.

Conclusion

With rising attacks on the healthcare sector for financial gain and geopolitical reasons, it is essential to implement and maintain robust security. Not only to protect the safety and essential performance of medical products, but also to safeguard interconnected systems that together deliver patient care.

References

All references checked and verified 28 October 2025.

1 International Organization for Standardization. ISO 14971:2019 Medical devices–Application of risk management to medical devices. Published December 2019. Accessed 17 September 2025. https://www.iso.org/standard/72704.html

2 Section 3305 of the Omnibus–Ensuring Cybersecurity of Medical Devices, amending the Federal Food, Drug, and Cosmetic Act (FD&C Act) by adding section 524B, Ensuring Cybersecurity of Devices (section 3305). 117th cong. Accessed 17 September 2025. https://www.congress.gov/117/bills/hr2617/BILLS-117hr2617enr.pdf

3 Ghafur S, et al. A retrospective impact analysis of the WannaCry cyberattack on the NHS. NPJ Digital Medicine. Published online 2 October 2019. Accessed 17 September 2025. doi.org/10.1038/s41746-019-0161-6. https://www.nature.com/articles/s41746-019-0161-6

4 Ralston W. The untold story of a cyberattack, a hospital, and a dying woman. WIRED. Published online 11 November 2020. Accessed 17 September 2025. https://www.wired.co.uk/article/ransomware-hospital-death-germany

5 Carroll, M. Patient's death linked to cyber attack on NHS, hospital trust says. Sky News. Published online 25 June 2025. Accessed 17 September 2025. https://news.sky.com/story/patient-death-linked-to-cyber-attack-on-nhs-hospital-trust-says-13388485

6 European Union Agency for Cybersecurity. ENISA threat landscape: Health sector. Published July 2023. Accessed 17 September 2025. https://www.enisa.europa.eu/publications/health-threat-landscape

7 Microsoft. US Healthcare at risk: Strengthening resiliency against ransomware attacks. Published 2024. Accessed 17 September 2025. https://www.microsoft.com/en-us/security/security-insider/threat-landscape/US-healthcare-at-risk-strengthening-resiliency-against-ransomware-attacks

8 Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC. Published 5 May 2017. Accessed 17 September 2025. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745

9 Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU. Published 5 May 2017. Accessed 17 September 2025. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0746

10 Medical Device Coordination Group. MDCG 2019-16 Rev.1 Guidance on cybersecurity for medical devices. Published July 2020. Accessed 17 September 2025. https://health.ec.europa.eu/document/download/b23b362f-8a56-434c-922a-5b3ca4d0a7a1_en?filename=md_cybersecurity_en.pdf

11 International Medical Device Regulators Forum. Software as a medical device: Possible framework for risk categorization and corresponding considerations. Published 18 September 2014. Accessed 17 September 2025. https://www.imdrf.org/documents/software-medical-device-possible-framework-risk-categorization-and-corresponding-considerations

12 American National Standards Institute, Association for the Advancement of Medical Instrumentation. ANSI/AAMI SW96:2023 Standard for medical device security–Security risk management for device manufacturers. Published 2022. Accessed 17 September 2025. https://array.aami.org/doi/book/10.2345/9781570208621

13 International Electrotechnical Commission. IEC 81001-5-1:2021 Safety, security and effectiveness in the implementation and use of connected medical devices or connected health software–Part 5: Security–Sub-Part 5-1: Security–Activities in the product lifecycle. Published 2021. Accessed 17 September 2025. https://www.iso.org/standard/76097.html

14 National Institute of Standards and Technology. NIST SP 800-218 Secure software development framework V1.1: Recommendations for mitigating the risk of software vulnerabilities (SSDF). Published February 2022. Accessed 17 September 2025. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf

15 Food and Drug Administration. Cybersecurity in medical devices: Quality system considerations and content of premarket submissions. Issued 27 June 2025. Accessed 17 September 2025. https://www.fda.gov/media/119933/download

16 Food and Drug Administration. eSTAR program. Current as of 3 December 2025. Accessed 30 December 2025. https://www.fda.gov/medical-devices/how-study-and-market-your-device/estar-program

17 Open Web Application Security Project. Top 10 web application security risks. Accessed 17 September 2025. https://owasp.org/www-project-top-ten/

18 Common Attack Pattern Enumeration and Classification. Accessed 17 September 2025. https://capec.mitre.org/

19 MITRE. Common Weakness Enumeration. Accessed 17 September 2025. https://cwe.mitre.org/

20 Fischer C, Hamming N. White Paper–IEEE PHD cybersecurity standards roadmap. IEEE PHD Cybersecurity Standards Roadmap. Published online 30 April 2019. Accessed 17 September 2025. https://ieeexplore.ieee.org/document/8703258

21 MITRE. Playbook for Threat Modeling Medical Devices. Published online 30 November 2021. Accessed 17 September 2025. https://www.mitre.org/sites/default/files/2021-11/Playbook-for-Threat-Modeling-Medical-Devices.pdf

22 International Medical Device Regulators Forum. Principles and practices for medical device security. Published 18 March 2020. Accessed 17 September 2025. https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf

23 Food and Drug Administration. Off-the-shelf software use in medical devices [guidance]. Issued 11 August 2023. Accessed 14 November 2025. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/shelf-software-use-medical-devices

24 International Medical Device Regulators Forum. Principles and practices for software bill of materials for medical device cybersecurity. Published 13 April 2023. Accessed 17 September 2025. https://www.imdrf.org/documents/principles-and-practices-software-bill-materials-medical-device-cybersecurity

25 Shimony E. Group policies going rogue. Cyberark. Published online 6 June 2020. Accessed 17 September 2025. https://www.cyberark.com/resources/threat-research-blog/group-policies-going-rogue.

26 Food and Drug Administration. Postmarket management of cybersecurity in medical devices [guidance]. Issued 28 December 2016. Accessed 17 September 2025. https://www.fda.gov/media/95862/download

27 International Medical Device Regulators Forum. Principles and practices for the cybersecurity of legacy medical devices. Published 11 April 2023. Accessed 17 September 2025. https://www.imdrf.org/documents/principles-and-practices-cybersecurity-legacy-medical-devices

28 International Organization for Standardization. ISO 81001-1:2021 Health software and health IT systems safety, effectiveness and security Part 1: Principles and concepts. Published March 2021. Accessed 17 September 2025. https://www.iso.org/standard/71538.html

29 National Electrical Manufacturers Association. ANSI/NEMA HN 1-2019 Manufacturer disclosure statement for medical device security. Published 8 October 2019. Accessed 17 September 2025. https://www.nema.org/standards/view/manufacturer-disclosure-statement-for-medical-device-security

8

Software Development

Coenraad Davidsdochter, MSc

Introduction

This chapter focuses on software development and validation in medical devices. Although it touches briefly on data management and governance, security, and usability of health software, other chapters provide deeper treatment of these topics. The author uses the term "software" for Software as a Medical Device (SaMD) and Medical Device Software (MDSW), including MDSW that is embedded on, drives, or influences the use of a hardware medical device, software accessories, and software components. For a discussion as to how SaMD and MDSW differ, see **Chapter 2** on Software as a Medical Device.

Standards and Guidance

Manufacturers should consider standards and regulatory guidance when implementing software development processes. This section introduces the most important standards and guidance documents.

The internationally accepted framework for lifecycle processes for medical device software is International Electrotechnical Commission (IEC) 62304.[1,2] This standard defines the processes, activities, and tasks manufacturers use to develop and maintain medical device software. This chapter outlines the sections of IEC 62304 that pertain to software development.

IEC 62304 defines software development lifecycle activities, except for design validation of the finished device (i.e., the process for confirming software specifications conform to user needs and intended uses).[1] Design validation is covered by IEC 60601-1[3,4] for the software part of medical electrical equipment, or IEC 82304-1[5] for software-only products.

For software that includes Artificial Intelligence (AI) or machine learning, additional activities need to be defined, such as those related to the data lifecycle of the AI model. In Europe, the AI Act (2024/1689) entered into force on 1 August 2024.[6] This horizontal regulation imposes mandatory development obligations on providers that place on the market or put into service high-risk AI systems. Multiple harmonized standards are in development at the time of this writing (e.g., in the areas of Quality Management Systems [QMSs], risk management, governance, and quality of data sets, logging requirements, transparency and information provision, human oversight, accuracy, robustness, and cybersecurity).

IEC 62304 defines processes, not development techniques. The sequence of development process steps described by IEC 62304 appears to suggest that a waterfall model be used (i.e., a sequence of steps to be followed in a specific order strategy, often represented in the classical V-model for sequential development).[1,2] Nevertheless, the standard does not prescribe any specific software development methodology approach, sequence, principle, or practice. The standard for QMSs, International Organization for Standardization (ISO) 13485:2016,[7] and the US Food and Drug Administration (FDA) guidance on design controls[8] appear to suggest that the design process be completed in the following sequence: planning, design input, design output, design review, verification, validation, and transfer. However, these documents are not intended to prescribe a specific chronological order for these activities.

Historically, (software) development departments felt burdened by the waterfall approach. When writing plans and requirements specifications, they had to document to the last comma and point before starting with the real work: coding. In contrast, an agile or iterative development approach allows them to perform system development and delivery in small increments.

Agile, a software development methodology, provides useful functions much earlier in the project, generates early feedback from strategic customers and users, allows developers to improve the functionality already on the market, and informs corrections to the original specification. Agile's principal purpose is to overcome the problem of discovering, at the end of a (large) development project, that the developed system does not meet the customers' real (and