ANSI/AAMI SW96: Raising the Bar for Medical Device Security Risk Management

Charles S. Farlow, Michelle L. Jump, Michael S. Seeberger, and Brian J. Fitzgerald

The recently published ANSI/AAMI SW96:2023, *Standard for medical device security—Security risk management for device manufacturers*,[1] seeks to address the challenges of managing security risks throughout the life cycle of a medical device. Developed by AAMI SM-WG05 (Device Security Working Group), SW96 is the first full standard on the topic of security risk management and updates content found in previous AAMI technical information reports (TIRs).

Why a Standard?

AAMI TIR57:2016, *Principles for medical device security—Risk management*,[2] provides guidance for medical device security risk management and was recognized by the Food and Drug Administration (FDA; recognition no. 13-83) soon after its publication. AAMI TIR97:2019, *Principles for medical device security—Postmarket risk management for device manufacturers*,[3] provides specific guidance for security risk management in the postmarket phase and also is recognized by the FDA (recognition no. 13-112).

Internationally, TIR57 has enjoyed a strong following among medical device regulators. Excerpts of TIR57 are included in many cybersecurity guidance documents, including those published by Health Canada[4] and the European Commission's Medical Device Coordination Group.[5] The security risk management process established by TIR57 is incorporated in the International Medical Device Regulators Forum's technical report, *Principles and Practices for Medical Device Cybersecurity*,[6] which was published in 2020. TIR57 also is listed as a relevant standard in *Medical device cyber security guidance for industry*,[7] published by the Australian Therapeutic Goods Administration in late 2022.

Although TIR57 and TIR97 have been widely successful, a TIR fulfills the narrow role specified in *AAMI Standards Program: Policies and Procedures*[8] "A technical information report (TIR) is a review of technical issues relevant to a particular technology and a statement of expert opinion."

TIRs provide timely information to industry stakeholders about a particular technical topic. TIRs often provide recommendations, which are statements that typically involve the use of the term "should". As a consensus standard, SW96 includes *requirements* for security risk management and therefore manufacturers can choose to conform to these requirements.

What Is Unique about SW96?

SW96 is based on the foundation established by TIR57 and TIR97. The standard's introduction references the Venn diagram illustrated in Figure 2 of TIR57 and states that it is "equally applicable to concepts presented in this document" (Figure 1).

Is this distinction still relevant? After all, more than six years have passed since the publication of TIR57. The recently revised FDA draft guidance, *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions*, includes the following statement in Section V.A.[9]: "The process for performing security risk management is a distinct process from performing safety risk management as described in ISO 14971:2019. This is due to the scope of possible harm and the risk assessment factors in the context of security may be different than those in the context of safety."

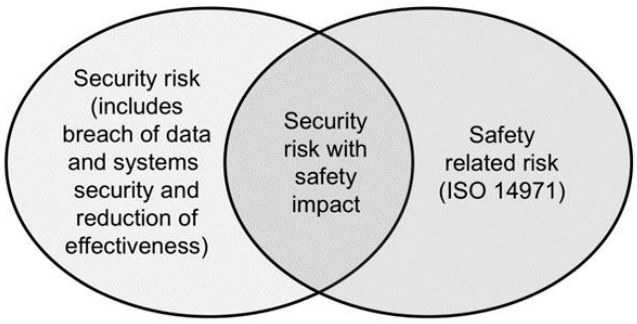

Figure 1. A Venn diagram showing the relationship between security and safety risks. Note: This figure appears as Figure 2 in AAMI TIR57:2016.[2]

Charles S. Farlow**, CISSP, is the senior director of program management and regulatory policy at MedSec in Miami Beach, FL. Email: charlesfarlow@medsec.com **Corresponding author

***Michelle L. Jump**, RAC, MS, is the chief executive officer at MedSec in Miami Beach, FL. Email: michellejump@medsec.com*

***Michael S. Seeberger**, MS, MBA, is a senior manager at Boston Scientific in Marlborough, MA. Email: michael.seeberger@bsci.com*

***Brian J. Fitzgerald** is a general engineer at the Food and Drug Administration in Silver Spring, MD. Email: brian.fitzgerald@fda.hhs.gov*

These two sentences, as simple as they may appear, lend credence to the Venn diagram of TIR57 and support the approach taken by SW96 to address the unique aspects of security risk management.

What's New in SW96?

One might notice that the security risk management process required by SW96 is similar to that recommended by TIR57. Other than specifying requirements, how does SW96 advance the state of the art for medical device security risk management?

Organization

The main body of SW96 is focused on specifying requirements with informative elements placed in notes or annexes. The standard defines a security risk management process that includes the following elements: security risk analysis (Clause 5), security risk evaluation (Clause 6), security risk control (Clause 7), evaluation of overall security residual risk acceptability (Clause 8), security risk management review (Clause 9), and production and post-production activities (Clause 10).

Many of these process steps retain foundational concepts established in TIR57. For example, in SW96, Figure 2 illustrates the communication of security risks with potential safety impact from the security risk management process to the safety risk management process. This figure also illustrates the communication of "security controls affecting safety" and "safety controls affecting security," which essentially translates to preventing the unintended consequences of a "siloed" application of risk control measures. The remaining subparagraphs of this section highlight important changes relative to TIR57.

Terms and Definitions (Clause 3)

One of the most important clauses in a standard is its terms and definitions. Many of the definitions incorporated in TIR57 and TIR97 have been revised to incorporate content from international standards, such as IEC 81001-5-1:2021.[10] Of note, the term "security" is defined in the context of the life cycle of a medical device.

General Requirements for Security Risk Management (Clause 4)

The security risk management plan (subclause 4.4) has been considerably expanded relative to TIR57. The plan addresses specific requirements for each step of the security risk management process. Subclause 4.5 requires the manufacturer to "establish, document, and maintain a system to monitor, collect and review supply chain information relevant to the security properties of the medical device." Subclause 4.6 specifies requirements for medical device manufacturers when the design or manufacturing of a medical device is subcontracted to a third party.

Security Risk Analysis (Clause 5)

Subclause 5.2 (Intended use and reasonably foreseeable misuse) requires manufacturers to ensure that reasonably foreseeable misuse "encompasses actions by threat actors, including exploits, which could cause harm, either intentional or unintentional." The standard also requires periodic review of reasonably foreseeable security risks to consider any new vulnerability disclosures.

Security Risk Management Review (Clause 9)

Clause 9 specifies requirements for the review process, whereas TIR57, Clause 8 (Security risk management report), is focused on contents of the associated *report*. Results of the security risk management review are recorded in the security risk management report and included in the security risk management file.

Production and Post-production Activities (Clause 10)

Clause 10 reflects a substantial expansion in content relative to TIR57. Clause 10 specifies requirements for *activities*, whereas TIR57, clause 9 (Production and post-production information), only specifies *information* to be collected in the production and post-production phase. Subclause 10.2.1 requires the manufacturer to establish a process for identifying and managing security incidents. Subclause 10.2.2 includes requirements to monitor a wide variety of information sources, including third-party suppliers of

software components specified in the software bill of materials (SBOM).

Supporting Annexes (Annexes A through F)

SW96 contains six new informative annexes that expand upon topics briefly discussed in the main body or that are of particular importance to practitioners in the security risk management field:

1. Annex A: Rationale
2. Annex B: The similarities and differences between security and safety risk management
3. Annex C: Security risk management report
4. Annex D: Threat modeling
5. Annex E: Third-party service organizations and security
6. Annex F: Security risk scoring based on likelihood of occurrence

Two of these annexes, Annex B and Annex D, are important because they address foundational concepts and threat modeling, respectively. Annex B contrasts the management of security risks with the probabilistic approach historically presented in ANSI/AAMI/ISO 14971. Subclause B.5 (Security attacks and the challenge of using probability) addresses this issue head-on and observes: "Fundamentally, a threat actor's capability and intent cannot be statistically modeled. The medical device manufacturer is often completely unaware of a product vulnerability until the threat actor attempts to exploit the weakness (commonly referred to as a 'zero-day attack')."

Subclause B.8 discusses the relationships between security risk management and usability engineering, including a new concept depicted in Figure B.4 (Interrelationship between safety, usability, and security).

Annex D reviews threat modeling principles and their application to medical devices. Threat modeling has become an important component of submissions and is now expected by regulators such as the FDA. Subclause D.4 provides guidance on how to integrate outputs of threat modeling in the security risk management process. Subclause D.5 provides an overview of several threat modeling methodologies, including STRIDE and Attack Trees.

Wrap-Up: Relevance of SW96 in the 'Post-Omnibus' Environment

On Dec. 29, 2022, President Biden signed the Consolidated Appropriations Act, 2023 (H.R. 2617),[11] into law. This act commonly is referred to as "omnibus." Section 3305 of the act amends the Federal Food, Drug, and Cosmetic Act, which establishes the legal framework within which the FDA operates, by adding new submission requirements to ensure the security of medical devices. SW96 addresses many Section 3305 requirements, including postmarket monitoring of vulnerabilities and exploits, coordinated vulnerability disclosure, postmarket updates and patches, and SBOMs.

TIR57 established a solid foundation for security risk management. SW96 advances the state of the art and provides a set of well-documented requirements for security risk management.

References

1. ANSI/AAMI SW96:2023, *Standard for medical device security—Security risk management for device manufacturers*. Arlington, VA: Association for the Advancement of Medical Instrumentation.
2. AAMI TIR57:2016/(R)2023. *Principles for medical device security—Risk management*. Arlington, VA: Association for the Advancement of Medical Instrumentation.
3. AAMI TIR97:2019/(R)2023. *Principles for medical device security—Postmarket risk management for device manufacturers* Arlington, VA: Association for the Advancement of Medical Instrumentation.
4. Health Canada. Guidance Document: Pre-market Requirements for Medical Device Cybersecurity. www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/application-information/guidance-documents/cybersecurity.html. Accessed April 17, 2023.
5. European Commission. *Guidance on Cybersecurity for medical devices*. https://ec.europa.eu/docsroom/documents/41863. Accessed April 17, 2023.
6. International Medical Device Regulators Forum. *Principles and Practices for Medical Device Cybersecurity*. www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf. Accessed April 17, 2023.
7. Australian Government. *Medical device cyber security guidance for industry*. www.tga.gov.au/sites/

default/files/medical-device-cyber-security-guidance-industry.pdf. Accessed April 17, 2023.

8. Association for the Advancement of Medical Instrumentation. *AAMI Standards Program Policies and Procedures*. www.aami.org/docs/default-source/standardslibrary/final-for-publication_aami-standards-program-policies-and-procedures-october-2021.pdf?sfvrsn=9c19c4ad_2. Accessed April 17, 2023.

9. Food and Drug Administration. *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions: Draft Guidance for Industry and Food and Drug Administration Staff*. www.fda.gov/media/119933/download. Accessed April 17, 2023.

10. IEC 81001-5-1:2021. *Health software and health IT systems safety, effectiveness and security — Part 5-1: Security—Activities in the product life cycle*. Geneva, Switzerland: International Electrotechnical Commission.

11. U.S. Congress. Consolidated Appropriations Act, 2023. www.congress.gov/117/bills/hr2617/BILLS-117hr2617enr.pdf. Accessed April 17, 2023.