

Collaborative Security for Medical Devices – Best Practices for Device Manufacturers and Healthcare Delivery Organisations

The proliferation of connected medical devices continues to introduce new cybersecurity risks that could impact patient safety and the security and privacy of patient data. To address these challenges, it is imperative that medical device manufacturers (MDMs) and healthcare delivery organisations (HDOs) collaborate effectively and prioritise medical device security (including design, implementation and maintenance) as a key priority for both entities. HDOs and MDMs can draw on guidance from the U.S. Food and Drug Administration (FDA), as well as industry standards from the National Institute on Standards and Technology (NIST) and key regulatory requirements like the Health Insurance Portability and Accountability Act (HIPAA) Security Rule as best practices.

As healthcare systems become increasingly digital and interconnected, ensuring that the availability, confidentiality and integrity of medical devices is protected is critical for patient safety and for the security and privacy of health data. Cyberattacks can lead to the malfunction of life-saving equipment, unauthorised access to sensitive patient data and overall disruption of healthcare services. Thus, a coordinated approach between MDMs and HDOs is necessary to mitigate these risks effectively. Simply put, medical device security should be considered a team sport.

Only recently have MDMs officially been charged with or expected to include security features within the design of medical devices, enabling these devices with default or optional security settings, configurations, etc., (e.g., drive encryption or secure authentication mechanisms like usernames and passwords or pin codes) where possible.

Simply put, medical device security should be considered a team sport, with a coordinated approach between MDMs and HDOs to effectively mitigate risks.

Concurrently, HDOs have been responsible for implementing and maintaining the security of devices within their organisations (e.g., understanding and configuring the embedded security settings and placing them in appropriate and secure network segments). However, as the devices and the environments within which they are being used continue to become more technically complex, achieving a secure state of being has become increasingly difficult. To that

end, some MDMs are seeing recent success in providing additional medical device security guidance and collaboration as a competitive advantage against their peers in the marketplace.

MDMs and HDOs can collaborate using the following strategies to ensure the safety of their patients and the security and privacy of their data:

1. **Document and share a roles-and-responsibilities matrix.** MDMs and HDOs must acknowledge that both parties play pivotal roles in designing, implementing and maintaining device security across various stages – from manufacturing through end-of-life disposal. Organisations should document and record specific roles and responsibilities each entity will play, along with service-level agreements (SLAs) which may already be contained within the contractual language and use those as a barometer for future analysis of how each organisation is complying with their specific tasks. This documentation can include, but should not be limited to:
 - The creation, updating and delivery of a manufacturer disclosure statement for medical device security (MDS2) and software bill of materials (SBOM)
 - Execution of periodic risk assessments
 - Identification of potential vulnerabilities
 - Patch management (e.g., device software, firmware and servers)
 - Regular operational maintenance on devices
2. **Utilise MDS2 forms, SBOMs and user manuals.** One of the easiest ways for MDMs and HDOs to share critical device security information is through the use of MDS2 forms, SBOMs and device user manuals. These documents continue to gain traction in the industry as the standard for security collaboration.
 - a. **MDS2:** The [newest version of the MDS2 form template](#) contains more than 200 cybersecurity questions and descriptions.
 - b. **SBOM:** While the community doesn't have a definitive template for the SBOM yet, this document should contain an inventory of all the software-related parts, pieces and components that make up the medical device and the platform it uses. This helps HDOs identify and track any risks and/or vulnerabilities inherently included within the device that may not be distinctly disclosed by the MDM as part of the product. This is very useful for disclosures of issues like zero-day vulnerabilities. MDMs should focus on creating, updating and delivering these documents, while HDOs should remember to ask for the documents, leverage their content to understand and implement devices securely, then add them to their accessible inventory for future use as needed.
 - c. **User Manuals:** This is the single most currently utilised document by HDOs and their medical device teams. Key considerations about how devices should be configured, default settings and accounts/passwords changed, user authentication integrations, etc., should be a key component of these manuals that can be better

utilised by HDOs to ensure the most optimal setups are occurring. Additionally, these manuals describe the needed preventive maintenance cycles that could be expanded to check for key security configuration and controls as part of the optimal operation to better ensure patient safety.

3. **Develop and distribute device whitepapers and implementation guidance.** Many MDMs have developed and distributed device-security white papers to help their customers and patients understand device cybersecurity at a higher level using layman's terms. These papers can provide directional intent, show broad capabilities and convey a commitment to security. Taking this idea one step further, MDMs and HDOs can collaborate to develop custom device implementation guidance, which can create a true competitive advantage when trying to sell devices to hospital systems. An extra advantage is gained by those who develop and maintain data flows and network diagrams detailing where and how electronic protected health information (ePHI) is shared over the hospital and/or vendor networks between the platforms, applications, databases, infrastructure, etc.
4. **Join and participate in information-sharing consortiums and working groups.** MDMs and HDOs should foster transparency between their organisations and seek to further their own education by joining and participating in information-sharing consortiums and working groups such as the Medical Device Information Sharing and Analysis Organization (MedISAO), Health Information Sharing and Analysis Center (H-ISAC), Healthcare Information and Management Systems Society (HIMSS), Medical Device Innovation Consortium (MDIC), Health and Human Services (HHS) 405(d) Program to align healthcare industry security practices, the Health Sector Coordinating Council (HSCC) Cybersecurity Working Group, Archimedes Center for Healthcare and Medical Device Cybersecurity, and more. These organisations each have differing viewpoints and objectives but can provide great platforms for both MDMs and HDOs to gather and share knowledge and work collectively on medical device security.
5. **Conduct joint cybersecurity risk assessments.** Organisations can partner to conduct periodic joint risk assessments leveraging tools like NIST's Cybersecurity Framework to determine vulnerabilities specific to integrated environments. This can be particularly helpful if the device or platform being assessed is technically complex and/or situated within a vendor's network within the health system. Teams can review the roles and responsibilities matrix, as mentioned above, alongside the MDS2 form to identify potential vs. implemented security configurations and options. Organisations can leverage a medical device security lifecycle assessment (see figure below) for projects such as this.

In our latest [Top Risks Survey](#), "Cyber threats" ranked as the top risk issue for healthcare industry board members and C-suite executives for the near term (two to three years ahead) and long term (a decade later, 2035).
6. **Coordinate incident response (IR) and resiliency planning with MDM partners.** Oftentimes, HDOs create their incident response plans (IRPs) in a vacuum and don't include other organisations in any planning or response or resiliency efforts. This is a mistake.

HDOs should leverage their relationships with their MDM partners to request assistance and support in the following IR-related activities:








- Easy identification and warm storage of device backup configurations
- Potential contracts and agreements for replacement devices in the event of widespread incidents
- On-demand technical support in the case of an incident
- Participation in tabletop exercises to test IR plans and coordination

7. **Leverage training, education and awareness.** Historically, MDMs designed devices; HDOs (biomed teams) implemented, used and maintained those devices; and, more recently, HDO cybersecurity teams protected those devices from cyber risks and threats. These teams simply didn't share knowledge, skills and/or experience. Going forward, these teams must work together to share best practices and determine how to best secure devices to protect patient health and safety and their data. Specific training and awareness components and programs can be leveraged from each source to collectively increase capabilities around securing and protecting medical devices. Easy examples of this include flyers and brochures, email newsletters, and even simple partnership commitment statements.

Enhancing cybersecurity in medical devices requires concerted efforts from both MDMs and HDOs. By adopting best practices recommended by regulatory bodies like the FDA and aligned with international standards such as the International Organization for Standardization (ISO) and NIST guidelines, organisations can build a robust defense against cyber threats. Collaboration is key. Sharing responsibilities, knowledge and strategies will lead not only to more secure products but also to safer healthcare delivery systems where patients' well-being remains paramount.

MEDICAL DEVICE LIFECYCLE REVIEW

The medical device lifecycle review program outlined below was developed with guidance from the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), the FDA pre/post guidance, and the HIPAA Security Rule to develop an assessment program for medical device security that covers key controls that constitute an effective medical device security program.

Function	Control Category
 Strategy & Governance	 Medical Device Security Program & Strategy Risk & Control Framework/Risk Management Processes Policies & Procedures Organizational Leadership & Team Integration Procurement Planning & Requirements
 Identify & Track	Asset Inventory, Categorization, and Prioritization Risk Assessment & HIPAA Risk Analysis Data Flow Documentation
 Protect	Access Control, Data Security, and Network Segmentation Manufacturer Disclosure Statement for Med Device Security (MDS2) Vulnerability & Patch Management Awareness and Training Device Handling Procedures
 Detect	Security Incident Identification, Logging, & Monitoring Loss & Theft Detection & Reporting Continuous Inventory Monitoring & Vendor Alerts
 Respond	Incident Response Plan Periodic Incident Response Plan Testing Incident Tracking & Handling Forensic Capabilities & Processes
 Recover	Disaster Recovery & Business Continuity Lessons Learned/Postmortem Exit from Lifecycle/Decommission



NIST, FDA, & HIPAA-Based Assessment

The assessment framework developed heavily leverages the NIST Cybersecurity Framework. This framework has been extremely popular due to its "attack focused" organizational structure. The FDA's pre/post medical device security guidance leverages CSF, and both control frameworks integrate with the HIPAA Security Rule standards and implementation specifications.

Additional Resources:

1. [Cybersecurity | U.S. Food and Drug Administration \(FDA\)](#)
2. [NIST Cybersecurity Framework](#)
3. [ISO 14971:2019; Medical devices — Application of risk management to medical devices](#)
4. [NEMA - Manufacturer Disclosure Statement for Medical Device Security \(MDS2\)](#)
5. [MedISAO \(Medical Information Sharing and Analysis Organization\)](#)
6. [H-ISAC \(Health Information Sharing and Analysis Center\)](#)
7. [HIMSS \(Healthcare Information and Management Systems Society\)](#)
8. [MDIC \(Medical Device Innovation Consortium\)](#)
9. [HHS 405\(d\) Program: A collaborative effort between the Health Sector Coordinating Council and the federal government](#)
10. [Health Sector Coordinating Council Cybersecurity Working Group](#)
11. [Archimedes Center for Medical Device Security](#)
12. [Principles and Practices for Medical Device Cybersecurity - IMDRF](#)
13. [There's a Culture Shift Happening in Medical Device Manufacturing. Are CISOs Ready?](#)
14. [Global Medical Device Company Assembles the Right Team and Microsoft Azure and IoT Solutions to Revolutionize Patient Care](#)
15. [Top Security Pitfalls for Medical Devices at Healthcare Providers](#)
16. [NIST Securing Internet Connected Medical Devices](#)

Contacts

Gareth Gruffydd

Managing Director

gareth.gruffydd@protiviti.com

Matthew Freilich

Director

matthew.freilich@protiviti.com

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned member firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, HR, risk and internal audit through a network of more than 90 offices in over 25 countries.

Named to the [Fortune 100 Best Companies to Work For®](#) list for the 10th consecutive year, Protiviti has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI).

© 2025 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. PRO 0525

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti®