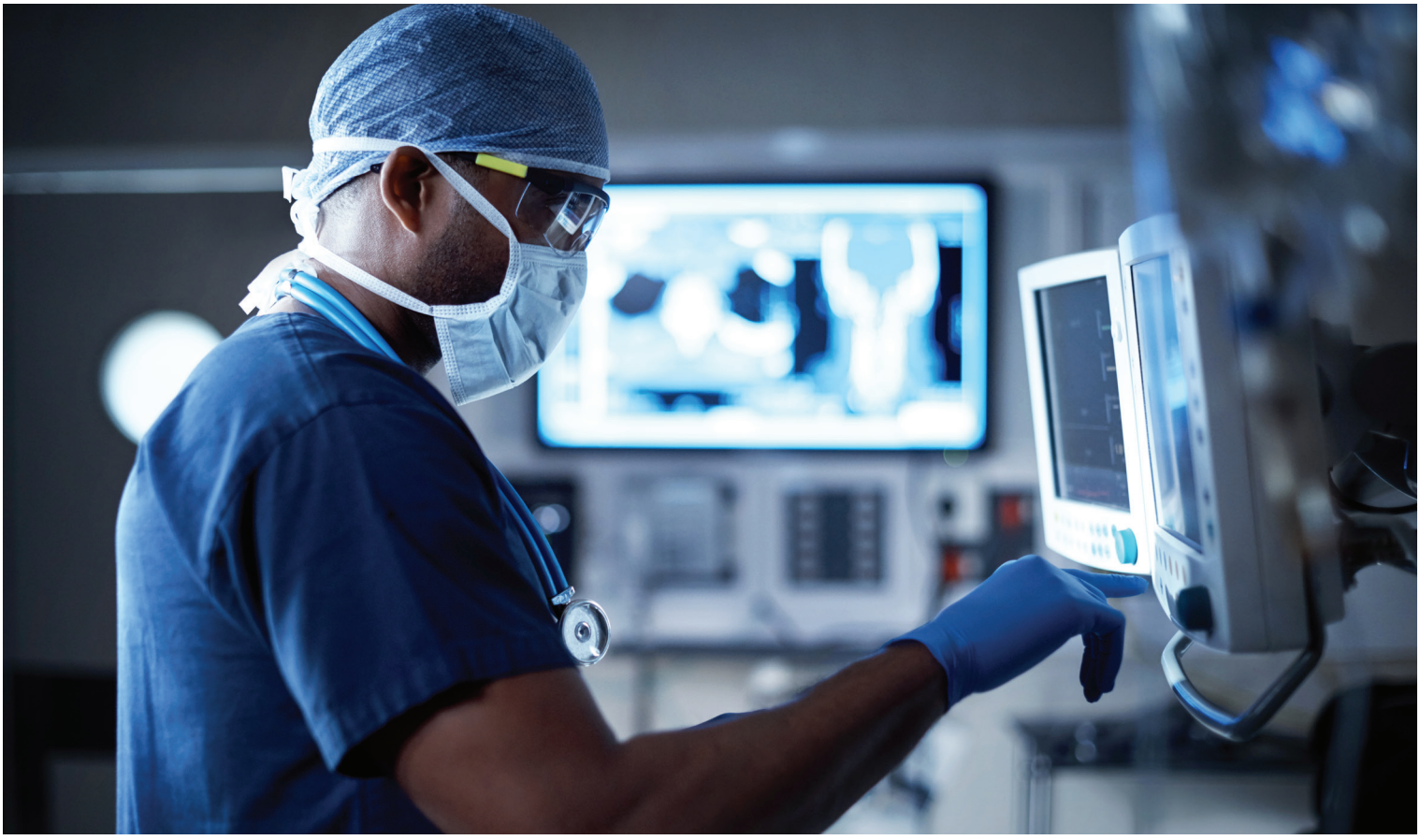
Crowe

July 2021

Connected medical device security: Why it matters

By Pamela S. Hrubey, CCEP, CIPP/US, Dr.PH, and Lucas J. Morris, CISSP



The rapidly increasing use of connected medical devices is revolutionizing patient and consumer interactions with health professionals and health systems. However, the transmission of sensitive data via such devices carries risks.

Organizations that use connected medical devices should perform necessary risk assessments to make sure that they are in compliance with various regulations, that sensitive data remains secure, and that hackers are kept at bay. By understanding the myriad regulations at large and by addressing the risks involved in using connected medical devices, organizations can mitigate their own risks and support their patients, clients, and consumers with confidence.

The internet of medical things

Manufacturers are producing more and more connected devices – commonly referred to as smart devices – that constitute the internet of things (IoT). From lightbulbs and kitchen appliances to door locks and thermostats, consumers eagerly have adopted the smart versions of common technologies.

One rapidly growing subset of the IoT includes medical devices, also referred to as the internet of medical things (IoMT). On average, U.S. hospitals report 10 to 15 connected medical devices per patient bed.[1] More than 350,000 connected medical devices can be running concurrently in larger hospital systems, individual patients maintain millions of their own devices, and within the next 10 years, more than 50 billion connected medical devices could be in use globally.[2]

Clearly, internet connectivity is here to stay with medical devices. Whether used in hospitals or clinics or at home, this revolution in medicine is allowing patients to gather data on their own health, and many devices offer doctors and care providers greater visibility into the health and lifestyles of their patients. Some devices even make more precise treatments possible.

While all this connectivity allows patients, providers, and medical professionals to enhance their health and services, it comes with additional risks. If hackers gain access to medical devices or their communication channels, they might be able to obtain patient data or negatively impact patient health. In fact, compromised devices potentially could cause severe injury or death. The U.S. Food and Drug Administration (FDA) has released several safety communications since 2013 highlighting instances in which medical devices were found to be vulnerable to hackers. The vulnerabilities included potential breach of patient data and risks to patients' health. For example, in 2019, the FDA warned of a vulnerability affecting a number of devices from various manufacturers that could lead to the loss of patient data or prevent devices from functioning.[3]

When breaches occur, responsibility is determined in several ways. According to the FDA, medical device manufacturers (MDMs) are responsible for the security of the devices they produce, healthcare delivery organizations (HDOs) are responsible for the security of their hospital systems, and both MDMs and HDOs share responsibility to address patient safety risks and to ensure the proper device performance. Those responsible for the security of the devices could face federal fines and class-action lawsuits, and they ultimately could suffer from reputational damage if security- and privacy-related issues become publicly exposed.

Regulatory risks and expectations

In many jurisdictions, health information is a class of data that requires regulatory guidance and control expectations, so MDMs and HDOs are required to maintain some accepted level of control and risk mitigation strategies specific to medical devices.

In the United States, one of the main entities that provides guidance for medical information is the Office of Civil Rights (OCR), which is the main enforcement arm of the *Health Insurance Portability and Accountability Act* (HIPAA). The General Data Protection Regulation (GDPR) focuses on data privacy and protection regulations as well as control expectations for all companies that handle, process, or transmit European citizens' personally identifiable data. Additionally, the FDA oversees and enforces the manufacturing requirements of medical devices used in the United States.

All these regulations have different impacts on and expectations for the controls and designs of medical devices. Therefore, it is crucial for organizations to understand how the regulations affect the configurations and vulnerabilities associated with medical devices.

HIPAA and protected health information

The *Health Insurance Portability and Accountability Act* is a federal law that requires U.S. medical organizations to protect patient health information from disclosure. Under HIPAA, medical device controls are not explicitly stated; however, controls are necessary to safeguard protected health information (PHI).

Because medical devices capture and transmit PHI, the manufacturing organization is considered a business associate under HIPAA, but it is not a covered entity. A business associate is defined as "a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity."[4] Covered entities include healthcare providers that "transmit any information in an electronic form in connection with a transaction for which [the Department of Health & Human Services] has adopted a standard," health plans, and healthcare clearinghouses.[5]

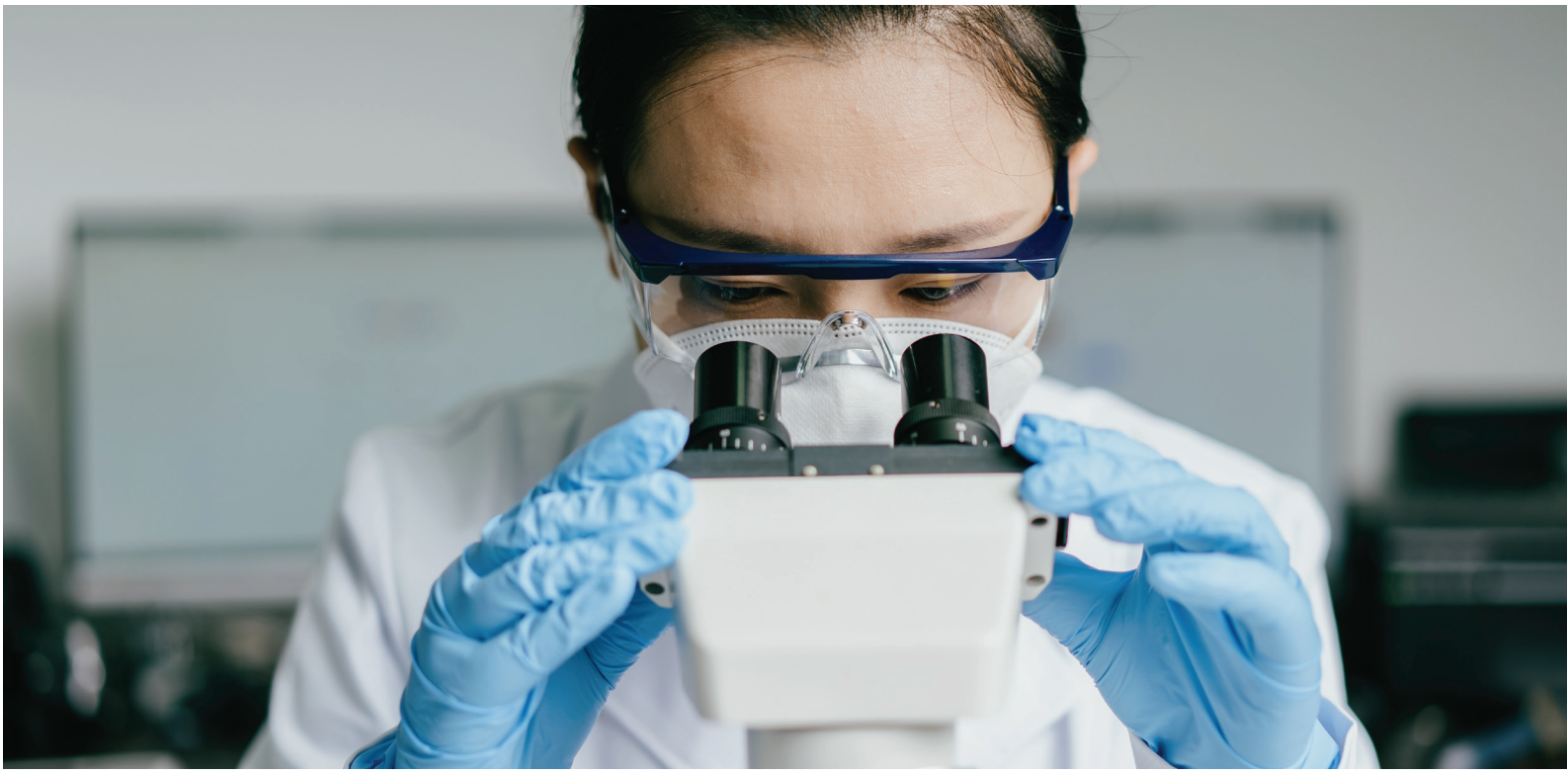
HIPAA has no specific controls or guidelines that business associates must adhere to when designing controls for medical devices within their organizations. However, when complying with HIPAA, organizations must understand the risk that medical devices can pose to the loss of PHI or to the other devices in their networks. Performing a risk assessment is the main avenue for exploring the risks associated with connected medical devices.

According to the National Institute of Standards and Technologies (NIST), a risk assessment is "the process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the nation, resulting from the operation of an information system."[6] Risk assessments also include threat and vulnerability analyses that can help guide the organizational decision-making process when implementing controls to address identified risks and potential vulnerabilities. For covered entities, both performing a risk assessment and understanding the scope and types of medical devices the organization uses are paramount concerns as they relate to HIPAA.

GDPR's wide-ranging protections

The GDPR is considered the most stringent set of regulations governing data use and protection ever implemented. The GDPR is intended to shore up the protections afforded to consumer data and reinforce consumers' fundamental right to privacy. The European Commission defines personal data as "any information that relates to an identified or identifiable living individual."[7] The GDPR protects personal data of European Union (EU) citizens and anyone who is in the EU, regardless of citizenship status.

In addition to protections established for personal data, the GDPR places special emphasis on information that is categorized as sensitive personal data. Generally, sensitive personal data includes personal data concerning health information, genetic data, biometric data, and personal data that reveals racial or ethnic origin. The GDPR applies to organizations in the United States that control or process personal information for European citizens. Because medical devices collect information that would fall into the GDPR-defined sensitive information category, organizations around the world need to consider if their medical devices will be used by European citizens.



GDPR regulations specifically require healthcare providers to obtain consent from patients for the organization to be able to process their personal data. The healthcare provider can bypass the user consent only if a "lawful basis for processing the personal data" exists. In order to obtain valid consent, organizations must meet several criteria. Consent must be freely given, specific, informed, unambiguous, and explicit. Additionally, the burden of proof for consent tracking is placed on the controller. The controller needs to have an audit trail around the consent, as consent can be revoked by the user at any time.

In terms of technical control expectations, GDPR requirements are similar to the HIPAA security rule. The GDPR is not specific about technical controls, and it does not require controllers or processors to follow any specific control frameworks or standards. However, the GDPR does state that organizations should use appropriate technical and organizational measures. As with HIPAA, the GDPR requires that organizations have a good understanding of the level of risk they assume when handling patient information. U.S. organizations concerned about GDPR risks should evaluate if the risk assessment for electronic protected health information (a process that should be in place as per HIPAA guidance) would also cover the definition of personal data, as defined in the GDPR.

In one example of a GDPR fine, the Data Protection Authority (DPA) in the Netherlands fined a public insurance agency for not having multiple factors of authentication on an online portal containing personal health data. The fined organization provided the online portal to employees to report employees' missed work dates due to general illness or pregnancy. The portal did not contain any information about the illnesses or conditions themselves. The DPA, however, ruled that this information constituted health data because it still provided information about employees' health. The DPA ordered the organization to conduct a privacy assessment and implement the results of the assessment before a certain date, with the threat of additional fines should the implementation not be completed on time. That the DPA considered seemingly innocuous data as health information demonstrates that any connected medical device falls under the GDPR should the device be used on a European citizen.[8]

FDA medical device regulations

The main focus of both HIPAA and the GDPR is to safeguard patients' privacy and to protect patients from losing data that belongs to them. But another level of regulation involves the devices themselves.

The FDA's Center for Devices and Radiological Health regulates organizations that manufacture, repackage, relabel, and import medical devices sold in the United States. FDA regulations, as opposed to HIPAA and GDPR regulations, are more focused on defining manufacturing processes to assure the safety of the patients who use medical devices.

All medical devices sold in the United States must be registered with the FDA through the establishment registration process. Medical devices generally are categorized into three classes (I, II, and III), and the regulatory scrutiny increases as the class does.

In general, the basic components of compliance for medical devices include the following areas:[9]

- Establishment registration
- Medical device listing
- Premarket notification 510(k) (unless exempt)
- Investigational device exemption
- Quality system (QS) regulation
- Labeling requirements
- Medical device reporting

QS medical device manufacturing requirements rely on an umbrella approach, similar to the current good manufacturing practices applied to most manufacturing companies. Because the regulations apply generically to all medical devices, the regulation is not prescriptive in nature but rather provides a known good manufacturing practices model that organizations must follow. Broadly, manufacturers should take care when developing their QS and consider which sections of the 21 CFR 820.5 QS regulation apply to their specific products and operations. Manufacturers are responsible for establishing requirements and procedures for all devices to ensure they are safe and effective and meet QS requirements.[10]

Medical devices that might have caused or contributed to the death or serious injury of a patient must be reported to the FDA under its medical device reporting program. The regulation supporting reporting is 21 CFR Part 803. Additionally, certain device malfunctions must be reported to the FDA.[11] The primary function of this regulation is to identify and remediate issues that might arise with medical devices in a timely manner, with the goal of protecting patients from related risks.

Sensitive data storage and transmission risks

Medical devices house and process sensitive information, so technical data protection mechanisms are essential components of medical device security. Because connected medical devices both transmit and store medical information, protecting health information becomes more difficult when medical devices use many different mechanisms to send and store the data they generate. Therefore, particular attention should be paid to sensitive data storage and transmission risks.

Data storage risks

Though some medical devices store patient data, users might not be able or allowed to gain direct access to the data files stored on the devices. However, the data might still be accessed through other means (such as a website, mobile app, or built-in interface). HIPAA does not require patient data to be encrypted, but it does consider encryption to be an addressable safeguard.

Addressable items must be implemented by the manufacturer if a risk assessment deems it necessary. Otherwise, manufacturers might not encrypt patient data while it is stored on medical devices, which could allow a hacker access to patient data if the hacker gains access to the device itself (physically or remotely).

Transmission risks

One of the most common functions a connected medical device performs is transmitting sensitive information to another device or dashboard where that data can be processed in an appropriate manner. Hackers approach the most common transmission protocols for this sensitive information to determine if they can gain unauthorized access to the PHI via vulnerabilities with the transmission protocol. Healthcare providers most commonly use the transmission standard for sensitive data called Health Level Seven (HL7).

HL7 was developed by Health Level Seven International, a not-for-profit organization that provides frameworks and standards for administering electronic health information. Two major versions of HL7 currently are in use: HL7v2 and HL7v3. HL7 has been implemented in 35 countries across the world, and in the United States, 95% of healthcare organizations use HL7v2.[12] HL7v3 is not as widely used, and it has yet to be formally approved by the American National Standards Institute. HL7v2 provides numerous customizable options when transmitting data; however, customization raises interoperability concerns when sharing data with other organizations. HL7v3's main function is to provide more structure for the process, limiting the amount of customization needed in order to transmit the necessary information.[13]

Because HL7 is the de facto standard for use in healthcare systems to transport sensitive patient data between different systems, connected medical devices need to have the capability to use HL7, even if that capacity is not by default. Organizations should be aware of HL7's limits, however. Developed in 1989, HL7v2's design did not include encryption as part of the protocol because the assumption is that encryption will be performed below the application layer. Therefore, native encryption should be implemented by organizations that adopt HL7 to prevent attackers from sniffing network traffic and extracting sensitive patient information out of the HL7 communication stream.

The HL7 protocol also does not perform integrity checking on data transported between devices. Integrity checking is important because it allows administrators to verify that the data being transmitted does not change when delivered. Without integrity checking, HL7 network traffic potentially could be captured and re-sent with incorrect or modified values of the data that is being transmitted. Falsified medical information sent from a medical device could lead to myriad issues for the patient down the line, including incorrect medical diagnoses or a false sense of security if medical data has been modified to make it seem that nothing is wrong.

In addition to HL7, connected medical devices can communicate using technologies such as Wi-Fi, Bluetooth, Zigbee, Z-Wave, radio-frequency identification, near-field communication, and others. These technologies allow devices to share information using application programming interfaces. They also can be used to manage devices from mobile apps or the cloud. Many connected devices, however, do not use the technologies to share sensitive information in a secure manner, including medical devices that transmit patient data or have remote control functions for administering a treatment.

The importance of risk assessments

Ultimately, an ounce of proactive prevention can help organizations successfully interact with the evolving IoMT world. By focusing on three main areas – penetration testing and red team services, security advisory, and security operations solution implementation – organizations can mitigate the risks involved with connected medical devices.

Crowe has worked with hundreds of companies across the United States and internationally to improve the quality of their cybersecurity posture through risk assessments, penetration testing, cybersecurity assessments, and the implementation of security and technology solutions. To learn more about how Crowe can help your organization, contact us today.

Learn more

Pam Hrubey
Principal
+1 317 208 1904
pam.hrubey@crowe.com

1. Julian Alvarado, "The IoT Within Us: Network-Connected Medical Devices," Software Integrity Blog, Synopsys, Sept. 14, 2018, https://www.synopsys.com/blogs/software-security/network-connected-medical-devices/
2. Kelly Rozumalski, "Working Together to Secure Our Expanding Connected Health Future," HelpNetSecurity, Oct. 6, 2020, https://www.helpnetsecurity.com/2020/10/06/working-together-to-secure-our-expanding-connected-health-future/
3. "URGENT/11 Cybersecurity Vulnerabilities in a Widely-Used Third-Party Software Component May Introduce Risks During Use of Certain Medical Devices: FDA Safety Communication," U.S. Food and Drug Administration, Oct. 1, 2019.
4. "Business Associates," U.S. Departmen= of Health & Human Services, May 24, 2019.
5. "Covered Entities and Business Associates," U.S. Department of Health & Human Services, June 16, 2017.
6. "Risk Assessment," Information Technology Laboratory, Computer Security Resource Center, National Institute for Standards and Technology.
7. "What Is Personal Data?," European Commission.
8. Kristof Van Quathem, "Dutch Supervisory Authority Imposes GDPR Security Standard for Processing Broadly Defined Health Data," Inside Privacy, Covington, Nov. 21, 2018, https://www.insideprivacy.com/health-privacy-dutch-supervisory-authority-imposes-gdpr-security-standard-for-processing-broadly-defined-health-data/
9. "Overview of Device Regulation," U.S. Food and Drug Administration, Sept. 4, 2020.
10. "Quality System (QS) Regulation/Medical Device Good Manufacturing Practices," U.S. Food and Drug Administration, Sept. 27, 2018.
11. "Medical Device Reporting (MDR): How to Report Medical Device Problems," U.S. Food and Drug Administration, Oct. 2, 2020.
12. "HL7 Version 2 Product Suite," HL7 International, https://www.hl7.org/implement/standards/product_brief.cfm?product_id=185
13. "HL7 Version 3 Product Suite," HL7 International, https://www.hl7.org/implement/standards/product_brief.cfm?product_id=186

crowe.com

CLS2299-007A