Connected Medical Devices: What Attorneys Need to Know

William H. Berglund
Tucker Ellis LLP
Cleveland, OH

Connected medical devices increasingly serve a vital role in improving the health and well-being of patients in all care settings. Connected devices have the potential to make patient care safer and more effective, yet, these devices can also pose significant privacy and security risks for health care organizations and safety risks to patients. Because of these risks, all stakeholders in the production and use of connected medical devices (manufacturers, health care providers, patients, and government regulators) must work together to ensure that these risks are properly assessed and managed. This article explores these issues and offers suggestions for what attorneys representing health care organizations can do to help manage this risk and improve patient care.

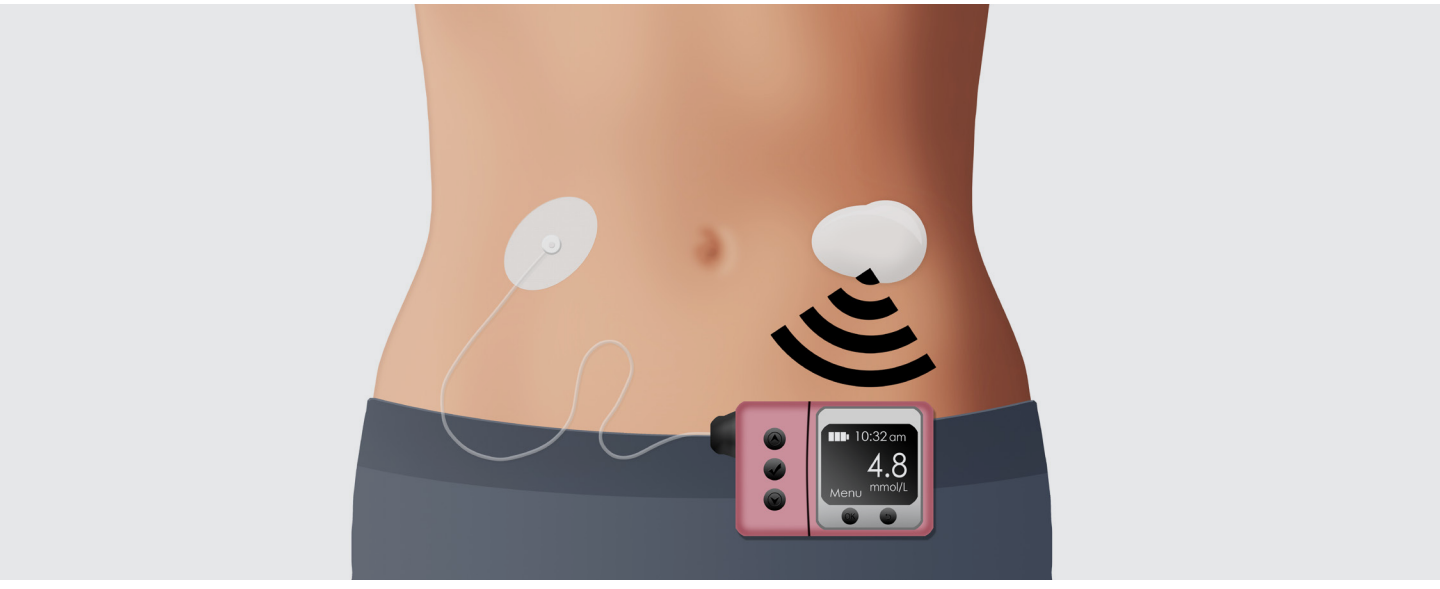
What Benefits Do Connected Medical Devices Provide?

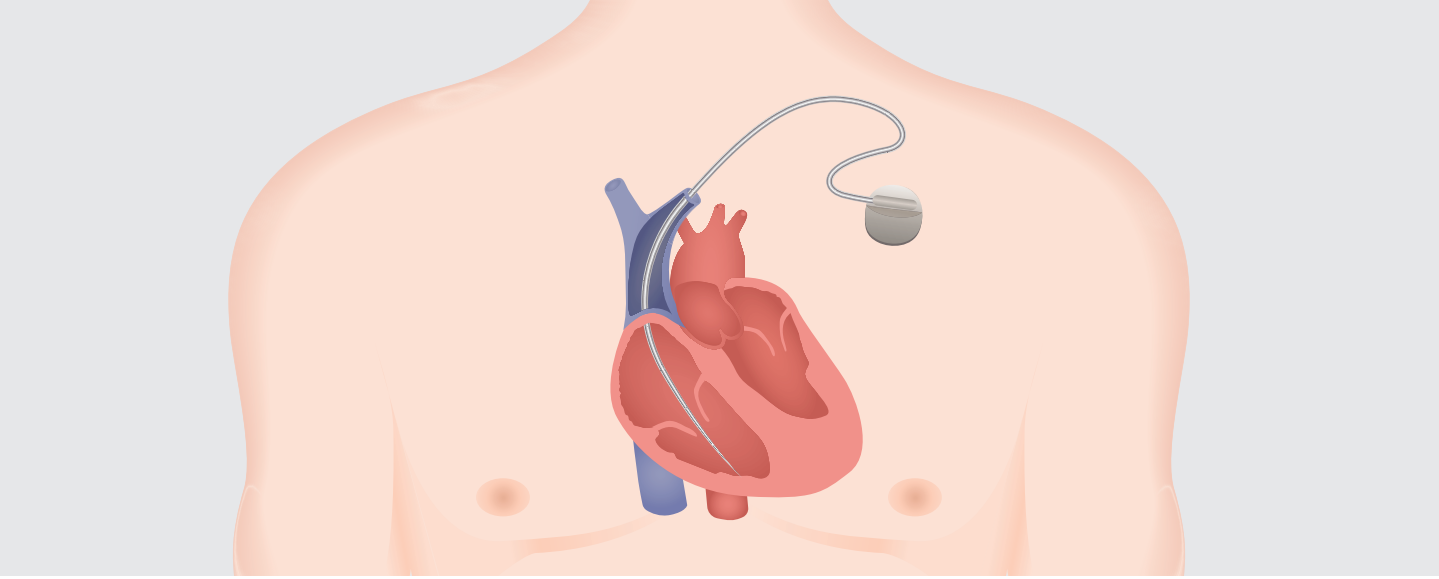
The Food and Drug Administration (FDA) currently regulates over 190,000 different medical devices, including basic medical supplies (bandages and hospital gowns), diagnostic tools (imaging machines), and implantable prostheses (heart valves and artificial pancreas).[1] With expanding technologies and design innovation, an ever-increasing number of medical devices are being connected to health care organizations' computer networks and integrated into patient care. Patients are also connecting personal devices that receive and transmit data through the Internet at home and elsewhere. Examples include implantable devices (cardiac pacemaker, cochlear implants), wireless insulin pumps and glucose monitors, other wearable devices that transmit data, scanning and imaging equipment (MRI, CAT scan), nurse call systems and other patient monitoring equipment, and mobile medical apps. New connected technologies are being designed every day.

Connected medical devices provide many benefits to both providers and patients. These devices can better personalize the delivery of health care to patients through the use of implantable and wearable devices that inject medication, provide reminders, and increase communication between patient and provider. Such devices increase the amount of data that allows providers to be more informed about their patients' health and adherence to treatment and allow for more interoperability as they can communicate with other devices and transmit data to the patient's electronic health record. Connected devices can also support better inpatient monitoring and the ability to respond more quickly in emergency situations. In sum, connected medical devices have the potential to lead to significantly safer and more effective patient care.

What Risks and Challenges Do Connected Medical Devices Pose?

The flipside of this increased connectivity is that, similar to computers and larger networks, these devices are vulnerable to cybersecurity breaches and can expose health care organizations and their patients to greater risks of stolen protected health information (PHI), impeded care and treatment to patients, and even physical harm to a patient.[2] In its June 2017 report, the Health Care Industry Cybersecurity Task Force noted: "The risk of potential cybersecurity threats increase as more medical devices use software and are connected to the Internet, hospital networks, and other medical devices."[3] Hackers increasingly view unsecured medical devices as a gateway into a health care organization's larger computer network.[4] Similar to other cybersecurity threats in the health care industry, vulnerabilities in connected devices can threaten the confidentiality, integrity, and availability of patient PHI and other data.[5] More importantly, however, these threats and vulnerabilities have the potential to cause patient injury or even death caused by the device itself failing to properly function





because it is compromised or the organization's health care operations in general are disrupted due to a larger network compromise.[6]

The Task Force's June 2017 report and a recent February 2018 draft report issued by the National Institute of Standards and Technology (NIST) on cybersecurity standardization for internet of things (IoT) technology provide a helpful summary of cybersecurity risks associated with connected medical devices. Some of the risks identified include:

- Failure of device manufacturers to provide timely security software updates and patches to medical devices and networks and to address related vulnerabilities in legacy devices.
- Malware that alters data on a diagnostic device.
- Denial of service attacks making a device unavailable for use.
- Exfiltration of PHI from the organization's computer network.
- Unauthorized access to the health care network, allowing access to devices and other segments of the network.
- Password problems leading to unrestricted access to the connected device.[7]

The Task Force also issued a series of recommendations for increasing the security and resiliency of medical devices and health IT in general. These recommendations included securing legacy device systems, improving transparency between device manufacturers and users to better understand vulnerabilities and how to implement security updates and patches, and the adoption of a full device lifecycle approach to combatting cyber threats.[8]

Both device manufacturers and health care organizations acknowledge that connected device security and the threat of a cyberattack are real problems. In a May 2017 survey conducted by the Ponemon Institute LLC, 56% of surveyed health care delivery organizations (HDOs) stated they believed an attack on a connected medical device they use was likely in the following 12 months.[9] Eighty percent of surveyed HDOs also said that medical devices are very difficult to secure.[10] Despite these results, only 15% of surveyed HDOs said their organizations were taking significant steps to prevent attacks against their connected devices.[11]

What Is the Legal and Regulatory Framework that Governs Connected Medical Devices?

Attorneys should familiarize themselves with several frameworks and guidance documents directed at increasing the safe and secure manufacturing and use of connected medical devices. In particular, the FDA's regulatory activity in this area and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and regulations are most relevant.

FDA Regulation and Guidance

The FDA is the primary federal agency responsible for regulating the safety and efficacy of medical devices. In the last five years, the FDA has issued final guidance documents that are designed to provide device manufacturers with recommendations for protecting connected devices from cybersecurity threats throughout the lifecycle of the device (design, development, and post-market risk management).[12] The FDA's guidance documents recognize that cybersecurity risk management must be a responsibility shared by device manufacturers, HDOs and providers, patients, and government agencies. They also stress that manufacturers must build in security controls when they design and develop devices, but then must also continuously monitor and address security risks once the device is on the market and is being used by providers and patients.[13]

Earlier this year, the FDA also released its initial *Medical Device Safety Action Plan*, a key focus of which is addressing cybersecurity of medical devices and the ever emerging threats and vulnerabilities.[14] As part of this plan, the FDA is considering requiring manufacturers to (a) build the capability to update and patch security into a device's design and demonstrate that as part of the

premarket process, and (b) develop a "software bill of materials" and provide it to the FDA and the device's customer and users, so the latter will be better equipped to manage the connected devices in their inventory and to be aware of the vulnerabilities related to those devices. The FDA's plan calls for updating its guidance documents to better protect against ransomware attacks and other moderate risks, as well as major risks that exploit a vulnerability in a device that could lead to a "multi-patient, catastrophic attack." The FDA also proposes the creation of a CyberMed Safety (Expert) Analysis Board, which would be a public-private partnership of members comprising a broad range of expertise with a focus on assessing vulnerabilities and risks and serving as a resource for device manufacturers, the FDA, and device users.[15]

HIPAA

Connected medical devices potentially implicate HIPAA to the extent they create, maintain, transmit, or receive patient electronic PHI (ePHI). Covered entities and business associates will need to incorporate connected devices into the organization's HIPAA compliance program. This includes conducting a risk analysis requiring "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of [ePHI] held by" the organization and then implementing a risk management plan that reduces those "risks and vulnerabilities to a reasonable and appropriate level."[16]

What Should An Attorney Do to Help Manage a Client's Risks Associated with Connected Medical Devices?

Managing cybersecurity risks associated with connected medical devices is a complicated task and should be conducted as part of the organization's overall security program. As part of this program, attorneys should work with their client health care organizations and providers to focus on several areas of cybersecurity risk:

- Ensure that a thorough inventory is conducted of all connected medical devices that are used within the organization. This inventory should document information about the vendor and purchasing history, connectivity, the software a device runs, the data it collects and transmits, and how these devices are accessed. This is the first step in managing device risks.
- Have a plan in place to manage legacy medical devices, including how vulnerabilities will be monitored and a system for installing security updates and patches. A similar plan should also be adopted for newer connected devices. If a legacy device is no longer being serviced by the manufacturer, assess the need for the device's continued use and determine how ongoing security risks can be managed. Make sure that a procedure is in place for destroying PHI and other sensitive data stored on a device when it is removed from use and disposed of by the client.
- Work with device manufacturers and other vendors to be aware of the latest threats and vulnerabilities to the devices in use and to assist in securing the devices throughout their lifecycle. Relatedly, advise clients that when they are purchasing new connected devices to work with vendors upfront to identify the security needed and to obtain sufficient security information about the devices to manage any vulnerabilities after they are put to use.
- Include a discussion of connected devices in any cybersecurity training of the client's staff. In particular, staff should be trained on proper password usage to ensure that only staff with proper authorization has access to connected devices.

Conclusion

Connected medical devices present many benefits to health care organizations and will continue to be used with increasing frequency to support patient care. With that increasing use comes corresponding increased privacy and security risks. All of the stakeholders discussed in this article play an important role in managing these risks and improving patient care. Attorneys representing health care organizations can serve a vital role in this area by being aware of the applicable legal and regulatory frameworks and by working with their clients to adopt organizational risk management practices that address the use of connected devices.

---

1 U.S. Food & Drug Administration, *Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health* (2018), at 1 (FDA Action Plan).

2 Interagency International Cybersecurity Standardization Working Group, Draft NISTIR 8200, *Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)*, National Institute of Standards and Technology (Feb. 2018), at 41-42 (NIST Draft Report).

3 Health Care Industry Cybersecurity Task Force, *Report on Improving Cybersecurity in the Health Care Industry* (June 2017), at 18 (Task Force Report).

4 Fred Donovan, *Medical Device Security Should Be Focus for Healthcare Providers* (Apr. 23, 2018), *available at* https://healthitsecurity.com/news/medical-device-security-should-be-focus-for-healthcare-providers (last accessed July 25, 2018).

5 Task Force Report, at 18-19; NIST Draft Report, at 41-42.

6 Task Force Report, at 18.

7 Task Force Report, at 18-19; NIST Draft Report, at 41-42.

8 Task Force Report, at 28-33.

9 Ponemon Institute LLC, *Medical Device Security: An Industry Under Attack and Unprepared to Defend* (May 2017), at 1.

10 *Id.* at 2, 7.

11 *Id.* at 1.

12 U.S. Food & Drug Administration, *Content of Premarket Submissions for the Management of Cybersecurity in Medical Devices*, Guidance for Industry and Food and Drug Administration Staff (Oct. 2014); U.S. Food & Drug Administration, *Postmarket Management of Cybersecurity in Medical Devices*, Guidance for Industry and Food and Drug Administration Staff (December 2016). The FDA has published additional information about medical device cybersecurity on its website. *See* https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm (last accessed July 25, 2018).

13 Suzanne Schwartz, M.D., *Managing Medical Device Cybersecurity in the Postmarket: At the Crossroads of Cyber-safety and Advancing Technology* (Dec. 27, 2016), *available at* https://blogs.fda.gov/fdavoice/index.php/2016/12/managing-medical-device-cybersecurity-in-the-postmarket-at-the-crossroads-of-cyber-safety-and-advancing-technology/.

14 FDA Action Plan, at 8, 13-14.

15 *Id.* at 13.

16 45 C.F.R. § 164.308(a)(1)(ii)(A)-(B).