The cybersecurity of digital medical devices: higher technological capabilities, higher likelihood of liability

Product Liability Alert

8 MAY 2019
By: Raymond M. Williams | Megan Krebs

Today, you would be hard pressed to find someone who is not monitoring steps, hours slept, water intake or calorie intake without the help of a fitness tracker or smartphone. In response, advances in technology monitoring one’s health have become commonplace. These advances have equally affected the medical device industry. Digital medical devices have integrated technology to offer patients, providers and medical device manufacturers with real-time updates about the patient’s medical condition.

These advances should be lauded. At the same time, however, it is useful to understand that, for medical device manufacturers and others along the distribution chain, the higher technological capabilities of digital medical devices bring with them a higher likelihood of liability.

These implications have played out in fictional accounts like the popular television show *Homeland*, in which a government official’s pacemaker was hacked by a terrorist organization. Although a dramatized account, this plot calls attention to the reality that medical device manufacturers must begin to think differently about potential liabilities caused by the increased use of digital medical devices.
Product liability is premised upon allocating liability to manufacturers for a product, or product component, that causes injury to an individual. In the case of a digital medical device, this chain of liability expands beyond the traditional confines of a manufacturer versus an injured individual.

For example, a digital medical device enables a patient’s protected health information (PHI) to travel from the patient, to the medical device, to the medical device company, which then forwards the data to the patient’s provider over a wireless network. In the event of a data breach or other cybersecurity event, a product manufacturer, software developer, medical device company, the healthcare provider and perhaps even wireless network providers could each find themselves potentially liable for the compromise of this patient’s PHI.

As technology keeps advancing, it is easy to see how this effect may ripple further. What if the device includes a smartphone app that enables patients to monitor their medical condition? What if the manufacturer uses cloud storage to catalog the patient’s PHI? Does the app developer, smartphone manufacturer or the cloud storage company open itself to potential liability if the patient’s PHI is compromised in a data breach?

As cybersecurity issues in healthcare continue to accelerate, the US Department of Health and Human Services (HHS) has increased its oversight of cybersecurity issues and its enforcement of penalties resulting from cybersecurity breaches. With respect to medical devices, the US Food and Drug Administration (FDA) recently closed its comment period for draft guidance on cybersecurity recommendations for premarket submissions of medical devices, and final guidance is expected shortly.

To prepare for potential new regulatory requirements, medical device manufacturers (we use this identification broadly) should take this opportunity to assess their compliance with the Health Insurance Portability and Accountability Act (HIPAA) and FDA’s Draft Guidance, then complete a Risk Management Plan. These steps will help manufacturers assess their own liability risk as more players — among them software developers, app developers and cloud storage companies enter the medical device industry.

Determining potential cybersecurity liability of medical device manufacturers

Recent HIPAA violations in the health care industry illustrate the potential liability that medical device manufacturers may soon face in the event of cybersecurity breaches. As of the time of this article, over 400 breaches, each affecting more than 500 patients are under investigation by HHS. Last year, HHS secured $28.7 million in judgments from its enforcement of HIPAA violations.

Medical device manufacturers are not immune from HIPAA penalties resulting from cybersecurity events. In the case of a breach, a medical device manufacturer may be liable under HIPAA as a business associate. Business associates now face increased liability under the Health Information Technology for Economic and Clinical Health Act (HITECH), which expanded HIPAA’s requirements, and increased government oversight of, these entities.

A medical device manufacturer also may be considered a covered entity under HIPAA. This will likely become more common as medical device manufacturers create digital products that transmit the patient’s PHI to his or her health care provider, and as manufacturers begin to perform more functions within the scope of HIPAA’s “covered entity” definition. For example, medical device manufacturers may contract with software or app developers that transmit or store PHI on the manufacturer’s behalf. This raises a separate question as to whether software developers, app developers, and other technology industry players may become liable under HIPAA as business associates. In the event of a cybersecurity event compromising a patient’s PHI, HIPAA liability would flow throughout the chain of business associates, and could impact technological companies that, until now, have had limited exposure to regulations like HIPAA.

These new business relationships set the stage for a new wave of product liability claims. Take, for example, the plot from Homeland: could the software developer for the pacemaker have been liable to the pacemaker user under product liability principles? Taking the plot a step further, what if the device used a smartphone app, and the app developer failed to push a real-time update to the device user that could have prevented the cybersecurity attack?

Recent FDA Draft Guidance provides the contours of how a product liability suit may proceed as medical devices become more advanced and manufacturers rely on other parties, like software developers, app developers, or cloud companies to develop products.

Shifting regulatory landscape: Draft Guidance on cybersecurity in medical devices
As medical device manufacturers rely on technology to develop products and open themselves up to cybersecurity attacks, the FDA is ensuring that manufacturers consider cybersecurity threats when designing their devices. On October 18, 2018, the FDA introduced draft guidance to address this topic. The comment period for this Draft Guidance closed on March 18, 2019.

The Draft Guidance recommends medical device manufacturers include cybersecurity device design and labeling as part of its premarket submission to enable FDA to evaluate the device's cybersecurity risk. To that end, the Draft Guidance establishes a tiered system for medical devices based upon their cybersecurity risk. Tier 1 devices are "higher cybersecurity risk" devices capable of connecting to other devices and networks, and in which a cybersecurity incident affecting the device could result in harm to multiple patients. A device that connects to the Internet and transmits PHI to health care providers may be an example of a Tier 1 device. By contrast, Tier 2 devices are those devices with no connectivity capabilities. As described below, the regulatory burden for a medical device will differ based upon its tier.

Device design

The FDA now recommends medical device manufacturers demonstrate the cybersecurity controls implemented in the device during the premarket submission process. Under the Draft Guidance, these controls should aim to (1) "identify and protect the device's assets and functionality" and (2) ensure the device's capability of detecting breaches. The Draft Guidance recommends security features to reduce unauthorized use, including passwords and multi-factor or biometric authentication. The medical device manufacturer also must ensure the device's code and data integrity, which should comply with the National Institute of Standards and Technology (NIST) standards. Lastly, though the Draft Guidance is silent as to its interaction with HIPAA, it nevertheless includes similar language requiring the manufacturer to maintain the confidentiality of patient PHI.

With respect to the device's detection capabilities, the FDA now expects medical devices to detect, log, and react to cybersecurity events in a timely manner. Tier 1 devices should include routine antivirus scans, and implement anti-malware, firewalls, or other parameters to limit the impact of cybersecurity events.

Device labeling

The Draft Guidance further delineates labeling changes for Tier 1 medical devices, potentially expanding manufacturers' labeling requirements and the failure-to-warn theories available to plaintiffs pursuing product liability claims. The FDA recommends, for example, that manufacturers include instructions on how to access the device's security features. The device should also include a cybersecurity Bill of Materials to inform users of the potential vulnerabilities of the device's component parts when interacting with other devices.

Perhaps one of the most important recommendations in the Draft Guidance is the request for manufacturers to include information "concerning device cybersecurity end of support." With such rapid technological advances, this recommendation highlights the likelihood that a patient's Tier 1 device may become outdated. At some point, the manufacturer may no longer push software updates or updated antivirus scans to these devices. Once a patient's device is out-of-date, the cybersecurity threat to the device will increase. At what point will the FDA no longer require a manufacturer to update the device's software, or ensure the software's code complies with NIST standards? What liability will a manufacturer face if a patient continues to use an outdated device? What role does the health care provider play, as the learned intermediary, in ensuring that his or her patients is no longer using an outdated device? The Draft Guidance does not answer these questions, but manufacturers should consider them when developing Tier 1 devices.

Device documentation

Under the Draft Guidance, premarket submissions for Tier 1 devices should explain how the device implements the recommendations discussed above, as well as risk management documentation that describes the cybersecurity threats that were considered in the device's design. By contrast, Tier 2 medical device manufacturers should expect to "include a risk-based rationale for why a cybersecurity design control was not necessary."

Cybersecurity risk management plan

In today's cyber world, companies MUST behave as if they will be attacked. With advanced medical device technology, a product manufacturer, software developer, medical device company, and perhaps even wireless
network providers could find themselves liable for the compromise of patient's PHI. Your only defense is a Cybersecurity Risk Management Plan. Medical device manufacturers must take steps to mitigate the harmful consequences of a possible attack that results in a data breach or a lack of services by preparing a Cybersecurity Risk Management Plan.

Understanding a broad risk mitigation strategy is the best approach to preparing your risk management plan. Hiring and retaining the best talent and having the right programs, policies and procedures in place will help mitigate against legal risk. As with all organizations, you will need benchmarking for your programs, policies and procedures. It is also key to have a basic analysis of the law done, which would include reporting requirements under cybersecurity laws, HIPAA and other guidelines as necessary. This may require a complete country/regional/state/local survey to understand the response requirements if you have a breach.

You will also need an Incident Response Plan in the case of a breach. The plan should be reviewed and if appropriate, tested by a third party consultant. Finally, understanding that a breach, even mitigated, may cost money, you should consider insurance to cover liability, the breach response, and fines. You should consider the difference in first party cost and third party cost and what protection do you have regarding third party vendors.

Conclusion

Medical device manufacturers should familiarize themselves with the Draft Guidance, including its adoption of NIST cybersecurity standards and new labeling recommendations around the manufacturer's provision of cybersecurity end of support for outdated medical devices.

Medical device manufacturers should take this opportunity to identify whether it may be a covered entity or business associate under HIPAA, and confirm its compliance and breach reporting obligations under HIPAA and HITECH to avoid any risk of liability in the event of a potential cybersecurity breach.

An earlier version of this article appeared on Law360 on May 8, 2019.

1 For purposes of this article, “medical device manufacturer” refers to all manufacturers of a digital medial device’s component parts or functions, including software or app developers, cloud storage companies, wireless network providers, and smartphone manufacturers. See Ray Williams & Jae Kim, Ready Or Not? Product Liability and Regulatory Implications for Digital Health Products, DLA Piper Product Liability Alert (July 2, 2018).
3 45 C.F.R. §§ 164.400-414.
4 45 C.F.R. § 160.103.
5 83 F.R. 52835; see also Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff (Oct. 18, 2018).
6 See id. at 10.
7 See id.
8 See id. at 20.
9 See id. at 21.

AUTHORS

Raymond M. Williams
Partner
Philadelphia | T: +1 215 656 3300
New Jersey (Short Hills) | T: +1 973 520 2550
raymond.williams@dlapiper.com

Megan Krebs
Associate
Philadelphia | T: +1 215 656 3300
megan.krebs@dlapiper.com