Bethany Corbin Attorney
bcorbin@wileyrein.com
Wiley Rein LLP, Washington DC

Security by design for the 'Internet of Medical Things' in the US

The Internet of Things ('IoT') is perceived as a new wave of technological development, with the ability to revolutionise consumer experiences and interactions. In the healthcare industry alone, IoT is expected to have an impact ranging from $1.1 trillion to $2.5 trillion per year by 2025, primarily from improved efficiency in treatment for chronic illness through remote monitoring and sensors[1]. The use of IoT devices in healthcare, however, raises important questions of patient safety and device security. As medical devices become increasingly connected, the endpoints from which an attack or data breach can occur multiply, and new technologies are being implemented faster than security systems can be updated. It is this tension between rapid technological advancement on the one hand, and data security and patient safety on the other, that has led to the development of a new trend: security by design. Bethany Corbin, Attorney at Wiley Rein LLP, details the necessity of security by design in connected medical devices with a focus on the 'Internet of Medical Things' ('IoMT'), how the US has progressed in regulating IoMT devices so far, and posits that security by design is essential not only to protect patients from physical harm, but also to reduce manufacturers' liability for insecure devices.

Security culture mindset

'Security by design' refers to the notion that networks, software and devices should incorporate security into their infrastructure at the outset, rather than reactively addressing security flaws at the back end[2]. Beginning with design conception, manufacturers are encouraged to weave fundamental security principles into their connected medical devices, with the overarching goal of strengthening device security before products hit the market. The US Federal Trade Commission has published guidance actively directing businesses to 'start with security,' and factor security into the decision-making process at every level - from development to sales[3]. Security by design thus promotes a collaborative approach to cyber security by purposefully engaging software and hardware manufacturers in the security conversation.

In the healthcare context, in December 2016 the US Food & Drug Administration ('FDA') issued guidance regarding the post-market management of cyber security in medical devices[4], which showcased the FDA's interpretation of statutory and regulatory requirements for managing cyber security vulnerabilities in healthcare devices that have already been approved by it and have been marketed to consumers. As part of this guidance, the FDA emphasised that device manufacturers should monitor and address cyber security vulnerabilities through the entire product lifecycle, including the design, production, distribution and maintenance phases[5]. In adopting this recommendation, the FDA recognised that the exploitation of medical device vulnerabilities can present a risk to patient health, thus requiring continual maintenance throughout the life of the product to guard against such exploits. Accordingly, the FDA has made clear that cyber security risk management is a shared responsibility between medical device manufacturers, information technology vendors, healthcare practitioners and health information technology developers.

The rationale supporting security by design is simple: by proactively considering security at every stage of device design and development, there will be available fewer insecure devices from which hackers can access personal health data or cause physical harm. In the context of connected devices, the goal of security by design is twofold: (i) to create a security culture that strengthens the impenetrability of devices that not only house personal health data, but also serve as weak links through which to access larger, more secure healthcare networks; and (ii) to increase patient safety and reduce the risk of physical harm, particularly with implantable medical devices.

IoMT cyber security

Although security vulnerabilities are not restricted to the healthcare industry, medical devices, and in particular IoMT, pose unique threats that can be addressed only through a comprehensive approach to cyber security. IoMT describes the network of smart medical devices that are connected to the internet (typically through Wifi) and have the ability to collect and exchange healthcare data. Such devices use embedded sensors to measure and transfer healthcare information through a network to data storage centres without human assistance[6]. In this manner, IoMT enables connected medical devices to interact with and gather data from physical environments and then transmit that data to other devices or people[7]. Recognisable IoMT examples include

1. Paez, Mauricio and La Marca, Mike, 'The Internet of Things: Emerging Legal Issues for Businesses', Vol. 43 (2016) N. Ky. L. Rev. p.29, p.33.
2. Miedema, Dr Theresa E., 'Engaging Consumers in Cyber Security', Vol. 21 J. Internet L. (February 2018) p.3.
3. Federal Trade Commission, 'Start with Security: A Guide for Business' p.2 (2015): https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf
4. U.S. Food & Drug Administration, 'Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff' (28 December 2016): https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf
5. Ibid. at p.4.
6. See Gorman, Leta E., 'The Era of the Internet of Things: Can Product Liability Laws Keep Up?', Defense Counsel J.: https://www.iadclaw.org/publications-news/defensecounseljournal/the-era-of-the-internet-of-things-can-product-liability-laws-keep-up/ (last accessed 24 June 2018).
7. See footnote 1, p.31.
8. Abbott & Chertoff Group, 'Why Medical Device Manufacturers Must Lead on Cybersecurity in an Increasingly Connected Healthcare System' p.2-3: https://www.chertoffgroup.com/files/docs/Chertoff_Abbott_WhitePaper_Final.pdf (last accessed 24 June 2018); Otto, Paul, 'Best Practices for Managing Cybersecurity Risks Related to IoT-Connected Medical Devices', JD Supra (12 March 2018): https://www.jdsupra.com/legalnews/best-practices-for-managing-23206/
9. U.S. Food & Drug Administration, 'FDA Safety Communication: Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter', FDA (9 January 2017): https://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm535843.htm
10. Weyland, Trevor, Medical Device Cybersecurity, Gallagher (19 May 2016): https://www.gallaghermalpractice.com/blog/post/medical-device-cybersecurity
11. See Weyland, Trevor, 'Medical Device Cybersecurity: Regulatory Oversight & Insurance Considerations', p.2 (September 2017): https://www.ajg.com/media/1699098/medical-device-cybersecurity-whitepaper.pdf; International Risk Governance Center, 'Governing Cybersecurity Risks and Benefits of the Internet of Things: Connected Medical & Health Devices and Connected Vehicles', p.10 (15 November 2016): https://infoscience.epfl.ch/record/229380/files/IRGC.%20(2017).%20Cybersecurity%20in%20the%20IoT.%20Workshop%20report.pdf
12. Ponemon Institute, 'Medical Device Security: An Industry Under Attack and Underprepared to Defend', p.1 (May 2017): https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/medical-device-security-ponemon-synopsys.pdf
13. Ibid. p.2.
14. Ibid.
15. Ibid.
16. Ibid. p.14.
17. See Mason Hayes & Curran, 'Untangling the Web of Liability in the Internet of Things', (19 May 2016): https://www.mhc.ie/latest/blog/untangling-the-web-of-liability-in-the-internet-of-things
18. See footnote 1, p.53.
19 See, e.g., footnote 6; Dean, Benjamin C., 'An Exploration of Strict Products Liability and the Internet of Things', p.19 (April 2018): https://cdt.org/files/2018/04/2018-04-16-IoT-Strict-Products-Liability-FNL.pdf; Butler, 'Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused By Hacked Devices?', U. Mich. J.L. Reform, Vol. 50 (2017), p.913, p.915–19.

continued

connected insulin pumps, pacemakers, glucose sensors and pill cameras.

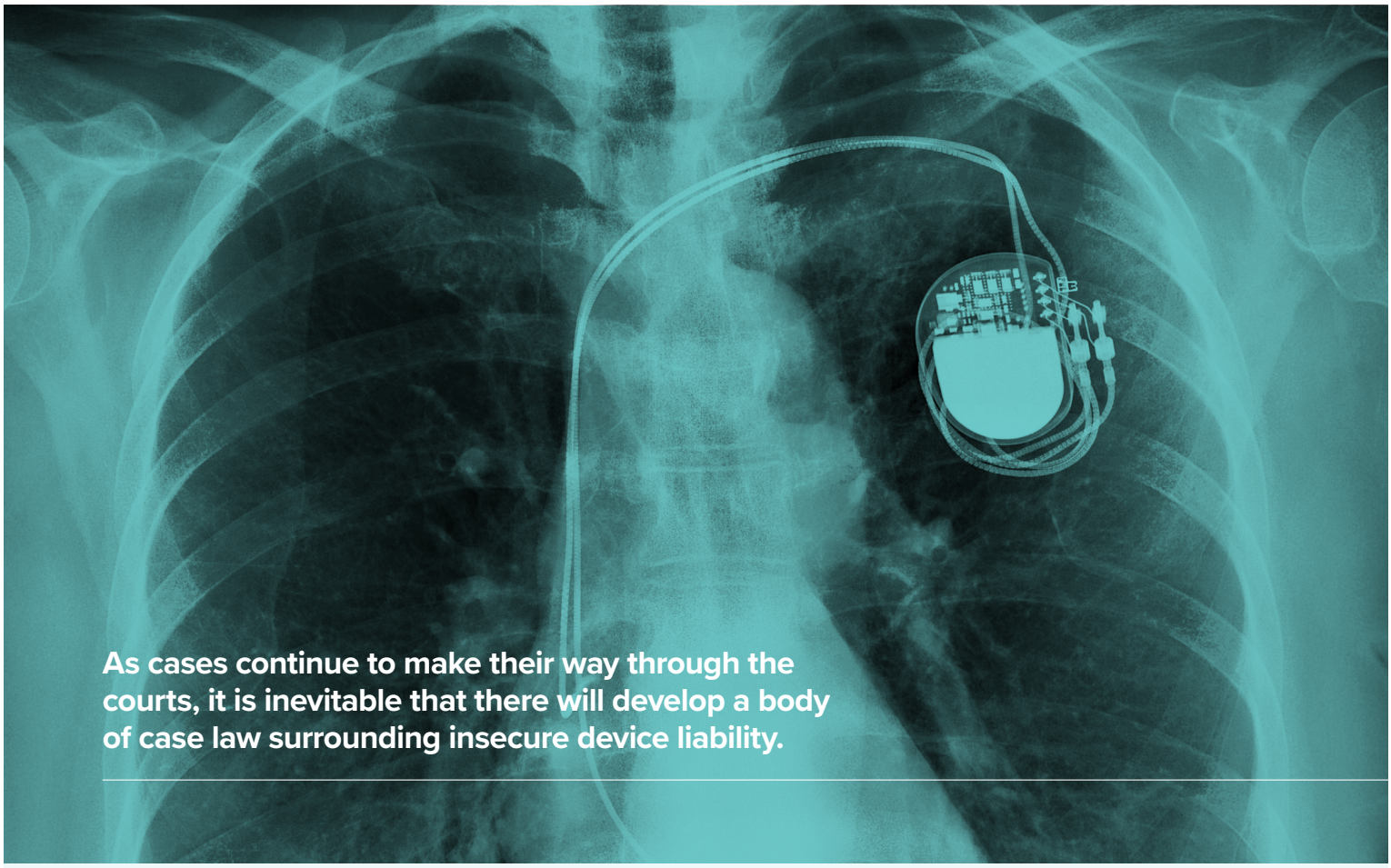
While IoMT is often lauded for the immense benefits that it confers on consumers - for instance, enhancing telemedicine and offering convenient medical monitoring for both patients and providers - it nonetheless presents challenging security issues that must be addressed throughout the product lifecycle[8]. IoMT interconnectivity enhances medical device vulnerability to security breaches and device hijacking, and further serves as a back door to hack other medical technology networks. Most importantly, malfunctions or hacking of IoMT devices may result in bodily injury - including death - for patients who use such products.

While actual instances of patient harm are rare, the ability to hack an IoMT device is no longer purely theoretical. In January 2017, the FDA published a safety communication warning patients with implantable cardiac devices that the Merlin@home transmitter could be hacked and result in unauthorised users controlling compromised devices[9]. Similarly, in 2011, a security expert hacked into an insulin pump at a Black Hat security conference[10]. Some experts therefore perceive connected medical devices as a weak link in provider security systems, with the potential not only to compromise system integrity and security, but also to impact patient safety negatively[11]. As the number of IoMT devices increases, the potential attack surface expands, creating new areas that are susceptible to cyber threats. Current legal and regulatory structures in the US, however, do not provide a comprehensive framework for IoMT security. Like a quilt, security and privacy regulations in the US for IoT are patchwork in nature, varying from industry to industry. The Health Insurance Portability and Accountability Act 1996 ('HIPAA') applies to certain IoMT devices used by covered entities in healthcare, but many uses of IoMT devices fall outside its scope. As a result, comprehensive IoMT guidance is still being developed. While numerous agencies, including the FDA, have issued guidance documents encouraging cyber security best practices, these guidelines have not been consistently implemented by IoMT manufacturers, developers and providers. Thus, the regulatory structures for IoMT are still a work in progress.

The need for security by design in IoMT

Given the lack of a comprehensive IoMT governance framework, it is crucial that manufacturers and developers approach connected medical devices from the perspective of security by design. To date, medical device manufacturers have not consistently emphasised security in their connected products, which places vulnerable devices on the market. A May 2017 study published by Ponemon Institute found that 67% of medical device manufacturers surveyed believed that an attack on their medical devices was likely, yet only 17% of those manufacturers had taken measurable steps to mitigate such potential attacks[12]. Similarly, 53% of device manufacturers noted that there was a lack of testing and quality assurance procedures, which could create vulnerabilities in IoMT devices[13]. According to those manufacturers, accountability for the security of medical devices was lacking, and cyber security risks were compounded by business pressures to release new devices as quickly as possible[14]. Further, device security after marketing may be virtually non-existent, with only 9% of device manufacturers confirming that they tested their medical devices annually[15].

By failing to embed security into the IoMT device at its outset, manufacturers not only invite medical device hacking and hijacking, but shift the burden of protection onto consumers. Consumers often do not possess the knowledge and resources to determine whether a medical device contains adequate cyber security protections, yet they must decide which devices to implant into their bodies or grant access to highly valuable health data. When faced with the stark reality that only 28% of respondents in the Ponemon Institute



As cases continue to make their way through the courts, it is inevitable that there will develop a body of case law surrounding insecure device liability.

study said that medical device testing was conducted before development and post-release[16], it becomes clear that security by design is necessary to reduce the risks of vulnerable code, particularly when such vulnerabilities could impact on an individual's access to life-saving treatment.

Security by design will not only ensure that medical devices are created with the most up to date security codes, but also promote consumer confidence in IoMT products[17]. As part of the security by design framework, manufacturers are responsible for conducting post-market tests of their medical devices, which will ensure timely and effective patching of vulnerabilities. This prevents medical devices from automatically becoming outdated and susceptible to hacking as technology progresses and new vulnerabilities are discovered. Further, pre-market testing will become more robust, and consumers can gain confidence in the products that they eventually purchase off the shelf.

Moreover, security by design may help to limit liability for manufacturers if their IoMT devices malfunction or are hacked[18]. Liability for IoMT device malfunctions and cyber attacks is unsettled, with the possibility that major parties - from manufacturers to healthcare providers - could shoulder at least partial responsibility. Numerous practitioners and scholars have speculated that accountability may eventually rest with device manufacturers under theories of negligence and product liability, although problems have been noted with the strict application of these doctrines in the IoT context[19]. As cases continue to make their way through the courts, it is inevitable that there will develop a body of case law surrounding insecure device liability. By implementing security by design principles, device manufacturers can defend against lawsuits by highlighting their emphasis on security at the design conception and production phases, and proving adequate pre and post-market device testing. These actions comport with existing FDA guidance.

Finally, security by design presents manufacturers with an opportunity to participate in establishing minimum cyber security standards with federal agencies, and contributing to dialogue on industry best practices. As manufacturers engage with cyber security vulnerabilities on a routine basis, they can contribute to public-private stakeholder collaboration on the development of cyber security regulations. The participation of manufacturers in cyber security discussions is critical to ensure not only that adequate regulations exist, but also that the regulations do not stifle IoMT innovation. Further, if medical device manufacturers have already adopted security by design, they may be in compliance with key components of future regulations on this topic. Therefore, security by design is a necessary investment to enhance patient safety and security, and to mitigate risks for device manufacturers and allow manufacturers to assist with defining standards in this evolving industry.

Conclusion

As cyber security threats develop, it is crucial that medical device manufacturers implement security protections in IoMT devices throughout the product lifecycle. Emphasising security during the design phase sets the tone for constant dialogue on security throughout product development, and ensures that IoMT devices are not rushed to market without adequate testing. In this manner, security by design increases patient protection and confidence in connected medical devices, and does not shift to consumers the entire burden of investigating device safety.

Further, security by design may help to reduce a manufacturer's exposure to liability if a cyber attack or device malfunction does occur. While courts and agencies continue to contemplate appropriate standards for IoMT, device manufacturers may contribute to this discussion and help to define cyber security best practices for connected medical devices.