



# The Vulnerabilities of Medical and Wearable Devices



Regulatory agencies have issued several guidances to help medical device manufacturers and users address the growing threat of cyberattacks on these devices.

Technological advances continue to transform healthcare delivery and how we track our personal wellness. For example, wireless medical devices such as pacemakers are being implanted in patients, accompanied by software that allows a healthcare provider to receive and transmit information directly to the device from a remote location. More commonly, people sport wearable devices such as smartwatches or fitness trackers to gather a variety of personal data for healthcare purposes and other purposes. While these devices are generally targeted to improve the user's health, they are not without risk. As medical and other wearable devices become increasingly interconnected with other systems, they become more vulnerable to both intentional and unintentional misuse, as well as cybersecurity attacks.

The term "cybersecurity" is used to cover a broad spectrum of context-specific adversarial challenges. Dan Craigen et al., *Defining Cybersecurity*, Tech. Innova-

- 

 ■ Caroline M. Tinsley, a partner in the St. Louis office of Tucker Ellis, defends leading product manufacturers in mass tort and product liability matters, with particular expertise in medical device and pharmaceutical liability. Ms. Tinsley manages complex and individual litigation for manufacturers and distributors of consumer products, pharmaceuticals, and medical devices. She is experienced in multidistrict litigation and class action product litigation in industries ranging from board games to medical devices and pharmaceutical products. Kelly A. Meredith is an associate of Tucker Ellis in St. Louis, where she focuses her practice on defending medical device and pharmaceutical companies against product liability and personal injury claims. In addition to defending product liability cases, Ms. Meredith has experience in working on intellectual property disputes, including multiple copyright infringement cases.

---

tion Mgmt. Rev., Oct. 2014, at 13–21. In the context of medical devices, cybersecurity is the process of preventing an unauthorized user from gaining access, modifying, misusing, or denying use to information that is stored, accessed, or transferred from a medical device to an external recipient. U.S. Food & Drug Admin., *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff* (Oct. 2, 2014); U.S. Food & Drug Admin., *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff* (Oct. 18, 2018) (updating 2014 ed.).

While fictional, the popular television show *Homeland* portrayed a medical device cybersecurity hack during which terrorists killed the vice president by remotely disabling his pacemaker. But the fear of medical device hacking by terrorists incited real-life action from former Vice President Dick Cheney, who, in 2007, had his doctors disable his pacemaker's wireless functionalities to prevent a possible assassination attempt. Dan Kloeffler & Alexis Shaw, *Dick Cheney Feared Assassination via Medical Device Hacking: 'I Was Aware of the Danger'*, ABC News (Oct. 19, 2013). The once seemingly futuristic exploitation of implanted medical devices is no longer science fiction; it has been successfully demonstrated in devices such as insulin pumps and pacemakers.

Likewise, in 2015, cybercriminals hacked into accounts of Fitbit users, and the hackers were able to gain access to users' data, including location history, showing where a person typically runs or exercises, and data showing the time that the user usually goes to sleep. Using numerous different mobile applications that collect and share information on users' location and movement pose the same risks. While seemingly harmless, the risks of disclosure of information with interconnected devices extends beyond having personal consequences to national security consequences. For example, Strava, an exercise application, initiated an update to its heat map of user activity in 2017, which allowed users to uncover details regarding the location of military personnel.

Although the risks of cybersecurity attacks through medical or wearable devices are not always foreseeable and cannot be eliminated entirely, manufacturers, regulators, and consumers can anticipate and manage many of the risks to prevent harm and the unnecessary disclosure of personal information.

---

■

In the context of medical devices, cybersecurity is the process of preventing an unauthorized user from gaining access, modifying, misusing, or denying use to information that is stored, accessed, or transferred from a medical device to an external recipient.

---

### Medical Device Regulation

The Food and Drug Administration (FDA), among other regulatory bodies, regulates the safety, effectiveness, and security of medical devices. These regulatory bodies have acknowledged the need for increased cybersecurity for medical devices by publishing guidance and recommendations for managing the risks to assist manufacturers with premarket submissions and postmarket risk-management plans. Specifically, the FDA has issued two guidance documents, one for premarket submissions, in 2014, updated in 2018 (*Premarket Submission Content Guidance, supra* (Oct. 2, 2014)); **Premarket Submission Content Draft Guidance, supra** (Oct. 18, 2018)), and one for postmarket management. U.S. Food & Drug Admin., *Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff* (Dec. 28, 2016). But who is ultimately responsible for preventing cybersecurity attacks on medical devices? Such responsibility is shared

equally by manufacturers, healthcare providers, and patients.

So, what exactly is a “medical device?” The FDA defines a medical device as follows:

an instrument... or other similar or related article... intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, or intended to affect the structure or any function of the body....

U.S. Food & Drug Admin., *How to Determine if Your Product Is a Medical Device* (Sept. 12, 2014). Ultimately, whether a device is a “medical device” depends on whether the manufacturer intends that the device be used for a medical reason that is not “achieved through chemical action or by being metabolized by the body.” *Id.*

This definition includes, for example, an infusion pump attached to a hospital bed, yet it excludes health and wellness applications that run on mobile devices and certain wearable devices, such as fitness trackers. The distinction between a medical device and wearable gadgets is not always so clear; increasingly, there are products that straddle the line between wellness wearable and medical device. Even though many wearable devices monitor a host of health information about the individual user, these devices are not regulated by the FDA. However, these devices can present similar security vulnerabilities and privacy concerns as medical devices, and unlike medical devices, they do not require the same level of certification and premarket efforts to protect consumers.

### Wearable Technology

The FDA considers most fitness-related wearables to be low-risk general wellness products that are outside the realm of the Federal Food, Drug, and Cosmetic Act. U.S. Food & Drug Admin., *General Wellness: Policy for Low Risk Devices, Guidance for Industry and FDA Staff* (Sept. 27, 2019). But manufacturers must consider federal regulatory frameworks as well as state-level regulations, which vary by jurisdiction. At the federal level, section 5 of the Federal Trade Commission Act vests the Federal Trade Commission (FTC) with authority to prohibit “unfair or decep-

tive acts or practices in or affecting commerce,” including unfair and deceptive privacy and security practices. In the context of interconnected devices, the FTC has stated that “this means that companies should maintain a reasonable security program and keep the promises they make to consumers concerning the security of their devices.” **Bur. of Consumer Protect., Staff Comments**, *In re Internet of Things and Consumer Product Hazards*, Docket No. CPSC-2018-007 (June 15, 2018). Accordingly, the FTC requires manufacturers to take reasonable steps to secure user information in accordance with their privacy policies. Vague and ever-changing privacy policies, however, leave a host of information vulnerable to misuse or hacking.

### Vulnerabilities of Medical and Wearable Devices

A vulnerability in a medical device is a weakness in its information system, security procedures, internal controls, or implementation capable of exploitation. “A threat” has been explained as “the potential for a vulnerability to be exploited,” and “the risk is calculated by consideration of the likelihood that a threat can occur together with a measure of the severity of any potential impact.” Patricia A.H. Williams & Andrew J Woodward, *Cybersecurity Vulnerabilities in Medical Devices: a Complex Environment and Multifaceted Problem*, 8 *Med. Devices (Auckl)* 305–16 (2015). The term “exploited” means that one or more vulnerabilities have been exposed either accidentally or intentionally, potentially affecting the essential clinical performance of a medical device or the system to which it is connected. **Post-market Management**, *supra* (Dec. 28, 2016). However, a vulnerability is not the same as a breach; a breach is the actual disclosure of protected information to an unauthorized user.

The increased connectivity and interoperability of medical devices has made medical devices increasingly vulnerable and susceptible to cybersecurity threats. The FDA has warned of some sources of, and incidents leading to, these vulnerabilities, including these:

- networked medical devices being infected and/or disabled by malware;

- the use of wireless technology (e.g., cell phones, tablets, hospital computers) to access patient data, monitoring systems, and implanted patient devices;
- uncontrolled distribution of passwords for privileged device access;
- failure to provide timely security software updates and patches to address vulnerabilities in older medical devices and networks; and
- security vulnerabilities in off-the-shelf software that do not prevent unauthorized device or network access (e.g., use of plain text code, lack of authentication, hard-coded passwords, poor coding).

Sonali P. Gunawardhana, **The Impact of Cybersecurity Vulnerabilities on Mobile Medical App Development**, *Med Device Online* (Dec. 4, 2015).

Recently, the FDA issued an alert about potential cybersecurity vulnerabilities, known as “SweynTooth,” which could affect medical devices with Bluetooth Low Energy (BLE), a technology found in medical and wearable devices that interconnects devices to communicate information. News Release, U.S. Food & Drug Admin., **FDA Informs Patients, Provers and Manufacturers About Potential Cybersecurity Vulnerabilities in Certain Medical Devices with Bluetooth Low Energy** (Mar. 3, 2020). If exploited, these vulnerabilities may allow an unauthorized user to take control of, crash, or shut down BLE devices, such as pacemakers, glucose monitors, insulin pumps, or stimulators, or even sizeable devices in healthcare facilities, such as electrocardiograms and monitors. This is just one of numerous regulatory communications over the past several years identifying cybersecurity vulnerabilities in medical devices and/or the wireless technology or communication software associated with these systems and devices.

Medical devices are vulnerable to attacks for a myriad of reasons. One reason is that unauthorized third parties or hackers have access to information, such as device manuals, patent databases, and device certifications, that may allow them to compromise a medical device. A second reason is that the large number of devices with access to a facility’s network, coupled with the fact that not all operating systems are compatible with one another, create opportunities

that could lead to misconfiguration and vulnerabilities through gaps in security. Likewise, already compromised medical devices can be used to attack other healthcare networks. Even seemingly beneficial features, such as reduced encryption, to allow for emergency access, present opportunities for attacks. Other reasons why medical devices or systems are particularly susceptible include outdated software, lack of basic security features to prevent tampering, and insufficient knowledge and training on cybersecurity and best practices among healthcare professionals. Williams & Woodward, *supra*.

Wearable devices present similar vulnerabilities. As with medical devices, wearable devices are interconnected to various other devices (e.g., computers, iPads, phones, cars, etc.) and use similar wireless technology. Additionally, users of wearable devices often contribute information to a centralized database, which, similar to other databases, are susceptible to attack by hackers.

### Cybersecurity and Attacks on Medical Devices

Current events and news outlets are constantly reminding us that cybersecurity threats are rampant. We frequently hear about data breaches exposing a variety of personal, financial, or governmental data. However, connectivity has extended cybersecurity threats beyond the computer and the information contained in it to medical devices and healthcare systems. In fact, a 2014 study revealed that 94 percent of healthcare institutions reported being victims of cyberattacks. Barbara Filkins, *Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon*, SANS Inst. (Feb. 2014). Although, to date, no one has hacked into a personal medical device to harm a patient, the following real-life events show that the possibility is no longer a far-fetched storyline: cybersecurity vulnerabilities in personal medical devices pose significant risks; and in the context of internal medical devices, they have made successful attacks possible.

**August 12, 2011:** A presenter at a security conference exposes the vulnerabilities of insulin pumps by demonstrating how



to hack into his own, although it required security expert knowledge and fairly close proximity to the pump. The presentation, even in 2011, stimulated conversation about the necessity of medical device manufacturers to rethink security measures to protect consumers from an attack. Morgen E. Peck, *Medical Devices Are Vulnerable to Hacks, But Risk Is Low Overall*, IEEE Spectrum (Aug. 12, 2011).

**April 25, 2014:** An article explores and exposes the vulnerabilities of hospital equipment and their high susceptibility to being hacked, including, but not limited to, insulin pumps, defibrillators, and hard-coded passwords in medical devices, used at a large chain of Midwest healthcare facilities. Kim Zetter, *It's Insanely Easy to Hack Hospital Equipment*, Wired (Apr. 25, 2014).

**July 31, 2015:** The FDA issues an alert for healthcare facilities to discontinue the use of a certain infusion system, due to cybersecurity vulnerabilities. Specifically, the system could be accessed remotely through a hospital's network, giving an unauthorized user access to the device and control to change the dosage of general infusion therapy the pump delivers. U.S. Food & Drug Admin., *Security Vulnerabilities in Infusion Pump Systems*, Medwatch, Medical Product Safety Information (May 13, 2015).

**June 2016:** A hacker gains access to "397,000 [] patient records from the internal network of a large database in Georgia, 210,000 patient records from a database somewhere in the Midwest (retrieved from a 'severely misconfigured network'), and 48,000 records located in Farmington, Missouri." Chris Nerney, *Hacker Puts 10 Million Stolen Health Records Up for Sale*, June 30, 2016. The hacker then put the information up for sale, requesting 750 bitcoins, the equivalent of around \$485,000 at the time. This is just one of many "ransomware" stories about a category of malicious software, referred to as "malware," which encrypts a user's disk drives and demands some form of compensation in return for critical data held hostage. Raj Mehta, *Health Held Hostage: Ransomware in the Health Care Industry*, MDDI Online (May 26, 2016).

**January 2017:** The FDA issues a Safety Communication after discovering that certain implantable cardiac devices could be

hacked through their home monitoring systems. U.S. Food & Drug Admin., *Cybersecurity Vulnerabilities Identified in Implantable Cardiac Devices and Transmitter*, Safety Communication (Jan. 9, 2017).

**May 2017:** United Kingdom and United States health systems, including medical devices located within a United States hospital, were infected by WannaCry ransomware. The attack compromised as many as 200,000 Windows systems, including those at forty-eight hospital trusts in the United Kingdom and an unnamed number in the United States. Thomas Fox-Brewster, *Medical Devices Hit By Ransomware for the First Time in U.S. Hospitals*, Forbes, May 17, 2017.

**March 2019:** The FDA issues a Safety Communication identifying cybersecurity vulnerabilities in a wireless telemetry technology used for communication among certain implantable cardiac devices, clinic programmers, and home monitors. U.S. Food & Drug Admin., *Cybersecurity Vulnerabilities Affecting Implantable Cardiac Devices, Programmers, and Home Monitors*, Safety Communication (Mar. 21, 2019).

**June 2019:** The FDA warns patients and doctors about the recall of certain insulin pumps, due to cybersecurity risks. News Release, U.S. Food & Drug Admin., *FDA Warns Patients and Health Care Providers about Potential Cybersecurity Concerns with Certain Insulin Pumps* (June 27, 2019).

**October 2019:** The FDA issues a communication identifying cybersecurity vulnerabilities for connected medical devices and healthcare networks that use certain communication software. News Release, U.S. Food & Drug Admin., *FDA Informs Patients, Providers and Manufacturers About Potential Cybersecurity Vulnerabilities for Connected Medical Devices and Health Care Networks that Use Certain Communication* (Oct. 1, 2019).

**January 2020:** The FDA issues a communication to raise awareness that cybersecurity vulnerabilities in certain clinical information stations and telemetry servers may introduce risks to patients while they are being monitored. U.S. Food & Drug Admin., *Cybersecurity Vulnerabilities in Certain Healthcare Clinical Information Central Stations and Telemetry Servers*, Safety Communication (Jan. 23, 2020).

## Best Practices to Manage Vulnerabilities and Cybersecurity Attacks

In response to these threats and attacks, as mentioned, the FDA issued a premarket submission guidance in 2014 and 2018, detailing premarket stage considerations addressing vulnerabilities. *Premarket Submission Content Guidance*, *supra* (Oct. 2, 2014); *Premarket Submission Content Draft Guidance*, *supra* (Oct. 18, 2018) (updating 2014 ed.). The agency also issued a postmarket guidance, covering mitigation, remediation, and other risk-management strategies, to aid in addressing medical device vulnerabilities and cybersecurity attacks on those devices. *Postmarket Management*, *supra* (Dec. 28, 2016).

The premarket phase considerations include the following: (1) identifying assets, threats, and vulnerabilities; (2) assessing the impact of threats and vulnerabilities on device functionality and end users; (3) assessing the likelihood of a threat and of a vulnerability being exploited; (4) determining risk levels and suitable mitigation strategies; and (5) assessing the residual risk and risk-acceptance criteria. *Premarket Submission Content Draft Guidance*, *supra* (Oct. 18, 2018). The manufacturer's premarket submission would include the premarket considerations conceived thus far, such as the hazard analysis and mitigation and design elements associated with the potential cybersecurity risks of a specific medical device; a summary of the plan for cybersecurity updates and patches; a matrix and summary showing and discussing cybersecurity controls and the potential risks; and instructions for the specific product with recommendations on how to use and secure the device properly. *Id.*

However, even after rigorous testing and risk assessment in the premarket submission phase, given the rapid pace of technology, medical device manufacturers must continuously evaluate the potential vulnerabilities of their devices and consider how to mitigate and remediate risks for marketed products. Williams & Woodward, *supra*. Mitigation is a risk-management strategy used to diminish the effect of a cybersecurity attack on medical devices and their correlated systems. *Id.* Remediation involves taking actions to

reduce the risk to a device's essential clinical performance to an acceptable level, including, but not limited to, finding a solution to combat a cybersecurity vulnerability, or using a compensating control, such as notifying the consumer about a temporary fix or other work-around solution. *Postmarket Management*, *supra* (Dec. 28, 2016). One common remediation strategy is to release "routine updates or patches," such as software, firmware, and hardware updates, that enhance the device's security and patch vulnerabilities that are linked to the device's controlled risk.

The FDA also issued the following other postmarket considerations: (1) monitoring cybersecurity information sources for identification and detection of vulnerabilities and risks, which may require auditing of the network and immediately reporting any security breach; (2) understanding, assessing, and detecting the presence and effect of a vulnerability; (3) establishing and communicating processes for vulnerability intake and handling; (4) clearly defining essential clinical performance to develop mitigations that protect, respond, and recover from the cybersecurity risk; (5) adopting a coordinated vulnerability disclosure policy and practice; and (6) employing mitigations that address cybersecurity risk early and before exploitation. *Id.*

The FDA also recommends the following best practices:

1. limit access to only trusted users through the use of passwords, usernames, smartcards, biometrics, automatic timers, and physical locks;
2. ensure that only trusted content is within the device and/or system by restricting updates to the same or using encryption;
3. "detect, respond, and uncover," by using procedures and features that alert security compromises, educate the end users on detections of security breaches, and provide methods for retention and recovery of devices (which are consistent with the National Institute of Standards and Technology "Framework for Improving Cybersecurity Infrastructure," i.e., "identify, protect, detect, respond, and recover");
4. create a structured and systematic approach to risk-management and qual-

ity management systems consistent with 21 C.F.R. part 820, which would include methods to identify, characterize, and assess a cybersecurity vulnerability and methods to analyze, detect, and assess threat sources;

5. be proactive—practice good cyber hygiene and reduce cybersecurity risks even when residual risk is acceptable;
6. remediate by finding an official or temporary fix to cybersecurity vulnerabilities to reduce the risk of compromise to essential clinical performance to an acceptable level;
7. keep in contact and maintain a solid, formal, business relationship with software vendors to ensure that they are providing you timely information about quality and security concerns that you can correct or prevent; and
8. incorporate elements consistent with the National Institute of Standards and Technology Framework for Improving Cybersecurity Infrastructure.

*Premarket Submission Content Guidance*, *supra* (Oct. 2, 2014); *Premarket Submission Content Draft Guidance*, *supra* (Oct. 18, 2018). See also Akin Gump Strauss Hauer & Feld LLP, Medical Device Alert, Jan. 28, 2016.

The FTC has also acknowledged the importance of cybersecurity measures as devices increasingly become interconnected and issued a recommendation that manufacturers get ahead of potential attacks. The FTC recommends the following best practices for manufacturers of consumer wearable devices to mitigate potential security and privacy risks, some of which are similar to those that the FDA recommends to manufacturers of medical devices:

- build security into devices at the outset, rather than as an afterthought;
- train employees on good security practices;
- retain service providers that are capable of maintaining reasonable security, and provide reasonable oversight to ensure that those service providers do so;
- implement a "defense-in-depth" approach by using multiple layers of security measures to defend against potential risks;
- implement reasonable control measures to limit unauthorized users from access-

ing devices, networks, or protected data stored in them; and

- monitor products throughout the life cycle and patch known vulnerabilities when feasible.
- Fed. Trade Comm'n, *Internet of Things: Privacy & Security in a Connected World* (Jan. 2015).

## Conclusion

The threat that a pacemaker will be hacked by foreign terrorists may be low, but the risk of devastating and life-threatening cybersecurity attacks in medical and wearable devices is significant and on the rise. Perhaps the benefits currently outweigh the risks for device users, but as technology advances to collect more sensitive data, it is important that manufacturers, regulatory bodies, healthcare providers, and consumers are informed of the ever-changing risks and work together to implement cybersecurity measures to mitigate these risks to protect consumers and their information. 