crowell moring

CLIENT ALERT

10 Ways to Reduce Cyberattack Risks on Internet-Connected Medical Devices

Sep.24.2021

Cyberattacks have become an omnipresent threat in our society, affecting every industry. On Friday, July 2, the biggest ransomware attack on record hit thousands of victims in at least 17 countries, including at least 200 companies in the United States. Hackers demanded $70 million in cryptocurrency to provide a decryption key. This attack followed on the heels of two high-profile ransomware attacks on U.S. infrastructure: the May Colonial Pipeline attack and the June attack on JBS, the world’s largest meat processing company.

This recent escalation in cyberattacks spotlights the risks to Internet-connected medical devices from ransomware, data theft, or hackers seeking to interfere with device function or effectiveness. Medical devices increasingly feature connectivity. Examples include implantable devices that export information to an external source (*e.g.,* pacemakers); wearable drug infusion pumps that export data, receive remote updates, and deliver “smart” doses (*e.g.,* wearable insulin or chemotherapy pumps); and any device that is connected to a hospital network (*e.g.,* IV therapy infusion pumps, robotic surgery devices, and MRI machines). Medical devices can be the end-targets of attacks, or serve as a cyber “back door” into hospital networks.

For these reasons, recent government and private sector developments in medical device cybersecurity warrant renewed attention. This article summarizes some of those recent developments and proposes various tools and techniques for manufacturers and providers to mitigate cybersecurity risks.

Potential Harm from Cyberattacks

Affected companies can suffer lost revenue due to system down time; the expense of restoring, recalling, or updating affected devices and networks; lost data and intellectual property; reputational harm; legal fees and litigation damages; and steep ransoms.[i] Companies may also be forced to defend against claims of harm when cyber vulnerabilities are simply identified, although plaintiffs may ultimately be unable to demonstrate standing to pursue litigation if no actual hacking attempt has been made or no injury has occurred.

For medical device manufacturers and healthcare providers, a cyberattack would not only expose vulnerable information but could also disrupt patient care. Just recently in April 2021, radiation treatments for cancer patients across the United States were delayed or disrupted due to a cyberattack on a Swedish healthcare software company. In May, Ireland’s health system was essentially disabled when it had to shut down its IT system due to a ransomware attack. These and similar attacks affect both patients and providers, and can even deter patients from seeking medical care. In studying the effects of the 2017 WannaCry global ransomware attack on the British National Health Service, researchers from the UK National Institute for Health Research found that there were 6% fewer admissions at hospitals infected with the WannaCry ransomware per day and 13,500 appointments cancelled over the week of the attack.[ii] The estimated financial impact was £5.9 m, or approximately $8.17 million today.

Recent Developments

Recognizing that “[c]ybersecurity is crucial for medical device safety and effectiveness,” the U.S. Food & Drug Administration (“FDA”) recently took the following steps:

- **September 2020:** FDA launched the Digital Health Center of Excellence within the Center for Devices and Radiological Health to foster digital health innovation and coordination on a variety of issues, including cybersecurity;
- **October 2020:** FDA issued a discussion paper, “Communicating Cybersecurity Vulnerabilities to Patients: Considerations for a Framework,” for public comment and use;
- **Beginning January 1, 2021:** FDA appointed Kevin Fu to serve as the first acting Director of Medical Device Cybersecurity in FDA’s Center for Devices and Radiological Health Office of Strategic Partnerships & Technology Innovation and the Digital Health Center of Excellence;
- **May 26, 2021:** FDA issued a report on its cybersecurity efforts in response to the National Institute of Standards and Technology’s call for position papers on standards and guidelines to enhance software supply chain security in accordance with the President’s May 12, 2021 Executive Order on Improving the Cybersecurity of the Federal Government (EO 14028); and
- **Late 2021:** FDA announced that it is targeting late 2021 to issue revised draft guidance on premarket submissions for management of cybersecurity in medical devices.[iii]

Additionally, on June 9, 2021, the U.S. Department of Health and Human Services’ (HHS) Office for Civil Rights published an email Cyber Alert: Updates on Ransomware and Critical VMware Vulnerability.

Industry is also working to stay abreast of evolving cybersecurity risks:

- **Fall 2020:** After United Health Services suffered a system-wide computer outage due to a suspected ransomware attack on September 28, 2020, Doylestown Hospital in Bucks County, Pennsylvania publicized its collaboration with a private vendor (Senasto) to develop a comprehensive cybersecurity program at the College of Healthcare Information Management Executives Fall Forum.
- **April 2021:** Sternum, an Israeli cybersecurity and analytics start-up, partnered with a major medical device company to provide cybersecurity through a real-time data analytics cloud-based security system for the Internet of Things (IoT), which will provide software updates to pre- and post-market devices.

10 Tips for Protecting Connected Medical Devices from Cyberattacks

Acting Director Fu recognizes that cyberthreats are increasingly sophisticated and healthcare is “fairly low-hanging fruit when it comes to cybersecurity.”[iv] Both manufacturers and healthcare providers should consider taking steps to proactively mitigate and address security-related risks to patient safety. For example, drafting a robust cybersecurity plan will help to ensure that medical devices function properly and securely, and that sensitive data stays protected. Some recommended steps that potentially impacted companies may consider include:

1. **Prioritize.** Cybersecurity should be part of quality management systems. FDA has denied premarket clearance based on cybersecurity concerns, and such concerns must be addressed both pre- and post-market.
2. **Know the rules**. HHS has specific guidance on cybersecurity and complying with requirements under the Health Insurance Portability & Accountability Act (“HIPAA”). For example, health care providers are subject to the HIPAA

Security Rule, which requires ensuring the confidentiality, integrity, and *availability* of health information and includes requirements to perform risk assessments and maintain backups of individually identifiable health information.

3. **Evaluate potential vulnerabilities and risks to patients.** Manufacturers should implement rigorous testing standards before marketing a product and engage in threat modeling. Providers should ensure that, once products are being used, they continuously monitor software updates and any other notices provided by the manufacturer.
4. **Incorporate multiple levels of protection.** Manufacturers and providers should use multiple levels of protection, such as software encryption for data and operations or multi-factor identification verification to the extent possible. As another example, employees may be required to use only secure networks using approved (and secured) devices.
5. **Develop an incident response plan.** Key stakeholders shouldidentify and outline the response and remediation actions that will be available if a cyberattack occurs. These actions may include both risk mitigation and attack response strategies.
6. **Plan ahead.** A rigorous training and continuing education plan can help to keep employees focused on data security.
7. **Outsource to the cyber experts.** Manufacturers and providers should explore vendor-provided security monitoring, planning, updating, or patching.
8. **Obtain legal advice.** Manufacturers and providers should consider seeking advice on security planning efforts and risk mitigation, development of corporate policies and training programs, responses to cyber incidents, and defense of litigation alleging present and/or future injury from cyberattacks. This may include assessing whether contracts and agreements should be modified to address or respond to cyber risks.
9. **Communicate.** All stakeholders should work to establish open lines of communication between manufacturers, vendors, and providers/systems. This may include establishing methods and guidelines for communications to patients.
10. **Stay up to date.** Key stakeholders should implement systems to track available resources and developments, including looking to what peers are doing in this space and evaluating FDA guidance on cybersecurity issues.

Conclusion

With society's increasing reliance on Internet-connected devices, cybersecurity's importance only continues to grow. Hacking incidents are unfortunately on the rise, affecting every industry, including medical and health care devices. The health care sector can and should take steps now to ensure the security of its medical devices to avoid inconvenient, costly, and dangerous outages and security breaches.

---

[i] Colonial Pipeline reportedly paid $4.4 million to regain access to its affected systems and JBS reputedly paid $11 million to do so. The Justice Department subsequently seized more than $2 million from the Colonial Pipeline hackers. The FBI discourages paying a cyber ransom, as there is no guarantee that an individual or organization will get its data back even if payment is made, and payment of a ransom encourages perpetrators.

[ii] Ghafur, S., *et al., A retrospective impact analysis of the WannaCry cyberattack on the NHS*, npj Digital Medicine 2, 98 (2019), at A retrospective impact analysis of the WannaCry cyberattack on the NHS | npj Digital Medicine (nature.com).

[iii] FDA CDRH and Medical Device Cybersecurity: Response to NIST Regarding President's Executive Order [EO] on Improving the Cybersecurity of the Federal Government [EO 14028] at 1-3 (May 26, 2021), https://www.fda.gov/media/149954/download

("FDA NIST Response"). The Communicating Cybersecurity Vulnerabilities to Patients: Considerations for a Framework discussion paper is available at Communicating Cybersecurity Vulnerabilities to Patients: Considerations for a Framework | FDA.

[iv] Greg Slabodkin, *Ransomware, other cyber threats mount as medtech industry tries to adapt*, MedTechDive May 25, 2021, at Ransomware, other cyber threats mount as medtech industry tries to adapt | MedTech Dive.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Andrew D. Kaplan
Partner – Washington, D.C.
Phone: +1 202.624.2699
Email: akaplan@crowell.com

Robbie Rogart Jost
Counsel – Washington, D.C.
Phone: +1 202.624.2556
Email: rjost@crowell.com

Sherrie Armstrong Davis
Counsel – Washington, D.C.
Phone: +1 202.624.2846
Email: sarmstrongdavis@crowell.com

Mimi S. Dennis
Counsel – Washington, D.C.
Phone: +1 202.624.2538
Email: mdennis@crowell.com