Cybersecurity in Medical Devices

Yuki Kinoshita
Clinical Research Associate
Clinical Research Strategies

Key stakeholders in the medical device industry, such as medical device manufacturers (MDMs), contract research organizations (CROs), sponsors, and hospital organizations, must recognize the importance of a vigilant approach to cybersecurity to ensure the protection of patient data, patient safety, and data integrity of medical devices.

Medical devices are increasingly becoming more advanced with new technologies and leveraging external connections to the Internet and hospital networks. Though these integrations can offer care that is more timely and convenient, the software behind the medical device can become vulnerable to cyber threats.[1]

The FDA defines cybersecurity as the process of preventing unauthorized access, modification, misuse, or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient.[2]

In August 2023, a joint research report by Health-ISAC, Finite State, and Securin, Inc. found that there was a 59% increase in vulnerabilities in medical products and devices from the previous year.[3] IBM Security released "Cost of a Data Breach Report" in 2023 and found that the average cost of a confirmed compromise of health-care data, also known as a breach, was $11 million, an increase of $1 million from the previous year.

Data breaches have disrupted healthcare delivery by rendering medical devices and hospital networks inoperable, delaying diagnosis and treatment.[4] Cyber-security breaches can put patients in harm's way, lead to the loss of patient trust, and cost companies millions of dollars. Due to increased cybersecurity threats and integration of Internet- and network-connected capabilities, the need for robust cybersecurity practices in the medical device industry must be prioritized.

Case in Recent Vulnerabilities

The healthcare industry is considered one of the most vulnerable sectors to cybersecurity attacks. Healthcare facilities and medical device companies have experienced countless attacks in recent years due to their size, technological dependence, and work in sensitive data.[5] In a 2024 survey, 92% of healthcare organizations reported having experienced at least one cyberattack, an uptick from 88% the year before.[6] The FBI reported in 2022 that 53% of connected medical devices and other Internet of Things (IoT) devices in hospitals had known critical vulnerabilities that put them at risk to cybersecurity attacks and data breaches.[7] While the statistics highlight the increasing vulnerabilities and cybersecurity threats to medical devices, real-world examples further illustrate the impact these threats have on hospitals and patients.

In May 2017, over 200,000 Windows systems across 150 countries were targeted in a coordinated global ransomware attack, known as WannaCry. The FBI considers WannaCry the first ransomware attack to target the operation of medical devices.[8] In addition to targeting medical devices, WannaCry largely targeted various companies and organizations, notably hospital systems in the United Kingdom and United States. The global ransomware locked all files in infected computers and demanded a ransom in Bitcoin for the user to regain control. Hospitals in the United Kingdom and United States were forced to cancel several thousand operations and appointments, thereby disrupting healthcare delivery for up to 48 hours.[9,10] The use of Windows systems and the connection to hospital networks left medical devices vulnerable to the attack and encrypted by the ransomware.

A prominent MDM confirmed that their radiology equipment was among the infected medical devices. The radiology equipment utilizes contrast agents to improve the quality of MRI scans.[11,12] According to their spokesperson, operations at the affected sites were restored within 24 hours and the MDM sent out a Microsoft patch for its Windows-based devices. The MDM recommended hospitals work with their IT security teams and the MDM's Technical Assistance Center to ensure continued support of the contrast-enhanced radiology procedures that were impacted.[13] Another MDM that was impacted by the attack did not confirm which of their medical devices were encrypted, but they similarly ensured to work on updates to patch the vulnerabilities in their affected products.[11]

The WannaCry ransomware attack exploited the vulnerabilities in the software behind medical devices and highlighted the importance of vigorous cyber-security measures.

Medical devices may also encounter cybersecurity issues from inadvertent data breaches caused by weak internal systems. In October 2023, an insulin pump MDM, issued an alert notice to its users that the health data of approximately 29,000 users may have been compromised in a data breach. This breach was connected to the recall of the remote controllers used with the insulin pump. The MDM sent emails to the insulin pump users requesting acknowledgment of the recall. It was within that email that, when the user clicked on the individualized link, it erroneously shared protected health information (PHI) with the MDM's website performance and marketing partners, including the users' IP addresses and whether they used the insulin pump and the associated remote controller. To address the breach, the MDM disabled their clickable tracking codes and requested that partners delete the logs of the users' IP addresses and unique URLs.[12]

FDA Cybersecurity Guidances

Though the FDA had issued cybersecurity guidances prior to the WannaCry ransomware attack, it was not until December 29, 2022, that cybersecurity standards for medical devices were established as legally enforce-able responsibilities. The Consolidated Appropriations Act, 2023, was signed into law and introduced an amendment to the Federal Food, Drug, and Cosmetic (FD&C) Act by adding section 524B, "Ensuring Cybersecurity of Devices," in section 3305, "Ensuring Cybersecurity of Medical Devices." Section 3305 provided the FDA with the authority to establish cybersecurity standards for premarket submissions—including 510(k), de Novo, HDE, PDP, and PMA—for any new medical device starting in March 2023, when the FD&C Act took effect. These standards outline the requirement of MDMs to submit plans to monitor, identify, and address cybersecurity vulnerabilities.

On June 27, 2025, the FDA issued the final guidance titled "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions."[14] In this guidance, the FDA provides high-level recommendations on medical device cybersecurity considerations, such as incorporating security risk management processes into the entire quality design and development of medical devices, as well as maintaining and supporting medical devices with regular updates.[15] Many of the devices impacted by WannaCry were running on outdated software, making them susceptible to the cyberattack.

Had cybersecurity standards for medical devices been established as legally enforceable responsibilities prior to 2017, one may ponder if the impact of WannaCry could have been minimized.

"Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions" also includes recommendations on what information to include in premarket submissions to ensure that marketed medical devices are adequately protected against cybersecurity threats. These recommendations include which information must be included in premarket submissions for devices with cybersecurity risk, like cybersecurity device design and labeling.

The "Select Updates for the Premarket Cybersecurity Guidance: Section 524B of the FD&C Act" guidance proposed updated recommendations regarding cybersecurity considerations for medical devices and the documentation in device premarket submissions.[15] Some of the proposed recommendations include having MDMs provide comprehensive documentation on how cybersecurity protections are designed into the device and how any vulnerabilities and exploits will be addressed.

CONCLUSION

Over recent years, cybersecurity attacks have increased in occurrence and severity. Medical devices are becoming more interconnected and more susceptible to these attacks and becoming increasingly susceptible to data breaches due to weak internal systems. Medical device companies, including MDMs, must adapt to this landscape and prioritize cybersecurity in the design and maintenance of their products.

CRS recognizes this challenge and its importance to patient data, patient safety, and data integrity of medical devices and can provide support in leading quality management system development, risk management, product requirements documentation, and validation of these types of systems. We are vigilant in addressing best business practices for cybersecurity functions and conformance to regulatory requirements in our processes as we know what's most important—the patients.

ABOUT THE AUTHOR

YUKI KINOSHITA
Clinical Research Associate

Yuki earned a bachelor's degree in public health with a clinical trials research concentration, magna cum laude, from Kent State University in May 2020, with membership in the Alpha Lambda Delta Collegiate Honor Society. She also received the University Award, President's Scholarship, and Trustee Scholarship.

Prior to joining CRS, Yuki worked for ALung Technologies and LivaLova, Inc. in clinical operations positions where she gained experience working on trial master files (TMFs), literature reviews, and clinical evaluation reports (CERs) for medical devices. She is dedicated to contributing to the CRS team and growing her skills in clinical research. In her spare time, Yuki enjoys pilates, hiking, and meditation.

REFERENCES

1. FDA. (n.d.). *Medical device cybersecurity: What you need to know.* U.S. Food and Drug Administration. https://www.fda.gov/consumers/consumer-updates/medical-device-cybersecurity-what-you-need-know.
2. FDA. (2025, June 27). *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions.*
3. McKeon, J. (2023, August 17). *Researchers Observe 59% Spike in Medical Device Security Vulnerabilities.* HealthITSecurity. https://www.techtarget.com/healthtechsecurity/news/366593925/Researchers-Observe-59-Spike-in-Medical-Device-Security-Vulnerabilities.
4. McKeon, J. (2023, July 24). *Average Cost of Healthcare Data Breach Reaches $11M.* HealthITSecurity. https://healthitsecurity.com/news/average-cost-of-healthcare-data-breach-reaches-11m.
5. Hales, M. (2023, December 12). *HHS Pushing to Strengthen Cybersecurity in Healthcare.* The HIPAA E-Tool. https://thehipaaetool.com/hhs-pushing-to-strengthen-cybersecurity-in-healthcare/.
6. Godard, R. (2024, November 27). *Healthcare Cybersecurity Statistics 2024.* IS Partners LLC. https://www.ispartnersllc.com/blog/healthcare-cybersecurity-statistics/.
7. FBI. (2022, September 12). *Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities.* (20220912-001). https://www.ic3.gov/CSA/2022/220912.pdf.
8. Riggi, J. (n.d.). *Ransomware Attacks on Hospitals Have Changed.* AHA Center for Health Innovation. https://www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed.
9. Smith, A., Smith, S., Bailey, N., & Cahill, P. (2017, May 17). *Why 'WannaCry' Malware Caused Chaos for National Health Service in U.K.* NBC News. https://www.nbcnews.com/news/world/why-wannacry-malware-caused-chaos-national-health-service-u-k-n760126.
10. Stevens, J. (2022, June 23). *The WannaCry attack and the NHS. Emerge Digital.* https://emerge.digital/resources/the-wannacry-attack-and-the-nhs/.
11. Alder, S. (2017, May 17). *WannaCry Ransomware Encrypted Hospital Medical Devices.* The HIPAA Journal. https://www.hipaajournal.com/wannacry-ransomware-encrypted-hospital-medical-devices-8811/.
12. Park, A. (2023, January 23). *Insulet alerts 29,000 Omnipod Dash insulin pump users to data breach linked to recall.* Fierce Biotech. https://www.fiercebiotech.com/medtech/insulet-alerts-29000-omnipod-dash-users-data-breach-linked-recall-notice.
13. Kovacs, E. (2017, May 19). *Medical Devices Infected With WannaCry Ransomware.* SecurityWeek. https://www.securityweek.com/medical-devices-infected-wannacry-ransomware/.
14. FDA. (2025, June 27). *Federal Register.* U.S. Food and Drug Administration. https://www.federalregister.gov/documents/2025/06/27/2025-11669/cybersecurity-in-medical-devices-quality-system-considerations-and-content-of-premarket-submissions.
15. FDA. (2024, March 13). *Select Updates for the Premarket Cybersecurity Guidance: Section 524B of the FD&C Act.*

ABOUT CLINICAL RESEARCH STRATEGIES

CRS is a US-owned and operated contract research organization and executive management consultancy for start-up and mid-size life sciences companies with a mission to improve their performance and provide a successful clinical research development plan and strategy. Our advisors have been everywhere – clinical research organizations, life science start-ups, medical device companies, and large pharma.