MedPro Group
a Berkshire Hathaway company

Risk Q&A

Managing the Internet of Things in Healthcare Organizations

Question

What is the internet of things (IoT), and does it present any risks in healthcare?

Answer

Healthcare has experienced significant growth in terms of clinical infrastructure, medical devices, and digital transformation.[1] Part of that growth includes the IoT, which is "a system of wireless, interrelated, and connected digital devices that can collect, send, and store data over a network without requiring human-to-human or human-to-computer interaction."[2] The IoT gives healthcare providers the opportunity to remotely monitor patients, make care decisions based on data, provide tailored treatment, and more.[3]

The IoT's market, which was $127.7 billion in 2023, is expected to rise to $289.2 billion by 2028.[4] Its explosion results from the IoT's ability to enhance patient care, significantly decrease healthcare costs via streamlining processes, automate regular duties, lessen the necessity for costly treatment, increase response times and enhance patient outcomes, maintain efficient data management, and more.[5] It also is used for hospital infrastructure management, as healthcare building management systems control the temperature, lighting, air quality, and more.[6]

More direct advantages of the IoT include how it is empowering patients and engaging them more with their healthcare. Patients are embracing wearable (and implantable) devices and apps to capture personal data, participating in telemedicine appointments, sending and receiving secure messages from their healthcare providers, accessing patient portals, and more.[7]

In the medical field, the IoT is referred to as the internet of medical things (IoMT). Some examples of the IoMT include remote patient monitoring, glucose monitoring, heart-rate monitoring, hand-hygiene

monitoring, blood pressure monitoring, depression and mood monitoring, Parkinson's disease monitoring, connected inhalers, ingestible sensors, smartwatches, smart contact lenses, robotic surgery, fitness trackers, devices needed for medical procedures and patient care, implantable devices, imaging devices, and medical diagnostic devices.[8]

Although the IoMT offers robust gains for patients and healthcare providers, it also ushers in many challenges and cybersecurity vulnerabilities, including inadequate authentication, external device access, software update concerns, unsecured network access, and inadequate device tracking.[9]

Organizations also face security risks with IoMT, including data privacy and security, data integrity and movement, management complexity, interoperability issues, authentication and authorization, ransomware attacks, outdated systems, availability, a compromised infrastructure, lack of staff training, device theft or tampering, lack of standardized protocols, and more.[10]

To tackle the challenges, cybersecurity vulnerabilities, and security risks associated with the IoMT, healthcare organizations should consider these high-level strategies:

- Develop an information technology (IT) governance policy/framework to minimize patient and organizational risks.
- Derive best practices from healthcare-specific regulatory frameworks for the organization.
- Have standardized protocols and interfaces in place so different devices are connected and operate seamlessly with each other, including the organization's electronic health record system.
- Continuously support a real-time inventory and monitoring system.
- Build role-based access controls and strong authentication controls into the organization's systems to avoid unauthorized access.
- Implement stringent security measures, including multifactor authentication, end-to-end encryption, network segmentation, Zero Trust architecture, firewalls, and intrusion detection systems.
- Ensure appropriate device management through security update administration, maintenance, and lifecycle oversight.

- Maintain updates on firmware and software to ensure devices are always running on the latest versions.
- Train healthcare staff on cybersecurity best practices, including proper medical device handling, user authentication, and more.
- Use secure communication protocols and encryption mechanisms to safeguard and store data.
- Work with device manufacturers to ensure regular security assessments, firmware updates, and compliance with the industry's best practices for cybersecurity.
- Keep long-term growth and technological advancements in mind when designing and planning systems in the organization's scalable infrastructure.[11]

Endnotes

[1] The Claroty Team. (2023, July 31). *Complete guide: Securing healthcare IoT devices*. Retrieved from https://claroty.com/blog/healthcare-iot-101-guide-to-the-internet-of-things

[2] Kelly, J. T., Campbell, K. L., Gong, E., & Scuffham, P. (2020). The Internet of things: Impact and implications for health care delivery. *Journal of Medical Internet Research, 22*(11), e20135. doi: https://doi.org/10.2196/20135

[3] Ibid.

[4] The Claroty Team, *Complete guide: Securing healthcare IoT devices*.

[5] Chunyan, L., Wang, J., Wang, S., & Zhang, Y. (2024, January 14). A review of IoT applications in healthcare. *Neurocomputing, 565*, 127017. Retrieved from www.sciencedirect.com/science/article/pii/S0925231223011402#sec0095

[6] Ibid.; The Claroty Team, *Complete guide: Securing healthcare IoT devices.*

[7] Ibid.

[8] Exein. (n.d.). *Cybersecurity risks of IoT in healthcare*. Retrieved from www.exein.io/blog/what-are-the-cybersecurity-risks-of-iot-devices-in-healthcare; ORDR. (n.d.). *10 internet of things (IoT) healthcare examples*. Retrieved from https://ordr.net/article/iot-healthcare-examples

[9] Exein, *Cybersecurity risks of IoT in healthcare.*

[10] Chunyan et al., A review of IoT applications in healthcare; Cylera. (n.d.). *Healthcare IoT security 101*. Retrieved from https://cylera.com/platform/healthcare-iot-security-101/#top; Roemer, Z. N., , Sumerauer, R. C., Sundquist, E. E., & Merhout, J. W. (2025). IT governance framework for the internet of medical things in the healthcare industry. *MWAIS 2025 Proceedings, 33*. Retrieved from https://aisel.aisnet.org/mwais2025/33/

[11] Exein, *Cybersecurity risks of IoT in healthcare*; Sahualla, M. (2025, April 24). *IoT compliance in healthcare: The essential guide*. Cylera. Retrieved from https://cylera.com/blog/iot-compliance-in-healthcare/; Airista. (2025, August 27). *What is IoT in healthcare*? Retrieved from www.airistaflow.com/resources/what-is-iot-in-healthcare/; Cylera, *Healthcare IoT security 101*; Coalfire Cybersecurity Team. (2023, October 23). *Guardians of IoT: Strengthening the security of IoT-connected medical devices in the healthcare industry*. Retrieved from https://coalfire.com/the-coalfire-blog/guardians-of-iot-strengthening-the-security-of-iot; Kelly, et al., The internet of things: Impact and implications for health care delivery