Acta Scientific MEDICAL SCIENCES (ISSN: 2582-0931)

Volume 9 Issue 5 May 2025

Mini Review

Hackable Health Care: The Vulnerabilities of Centralized Medical Technology in Modern Health Systems

Lisa Miron JD and Robert Oldham Young*

Department of Research, Innerlight, Biological Research and Health Education Foundation, USA

***Corresponding Author:** Robert Oldham Young, Department of Research, Innerlight, Biological Research and Health Education Foundation, USA.

Received: December 11, 2024

Published: April 14, 2025

DOI: 10.31080/ASMS.2025.09.2072

Abstract

The increasing reliance on centralized electronic systems and Internet of Things (IoT) devices in healthcare has created new vulnerabilities, exposing health systems to cyberattacks, privacy breaches, and data manipulation. This article explores how centralized systems risk overshadowing doctor-patient relationships, prioritizing monitoring and control over actual health outcomes. It highlights major examples of IoT security breaches, the implications of wearable device vulnerabilities, and the risks posed by interconnected medical technologies. Finally, it proposes solutions to enhance cybersecurity, protect patient data, and promote detoxification strategies, including the use of MasterPeace Zeolite Z™ and SOLergy Sea Minerals™, to mitigate the effects of IoT exposure.

Keywords: Hackable Health Care; IoT Security; Medical Technology Vulnerabilities; Cybersecurity in Healthcare; Doctor-Patient Relationship; MasterPeace Zeolite Z™; SOLergy Sea Minerals™

Introduction

The digitization of health care has brought unparalleled advancements in patient monitoring, diagnosis, and treatment. However, this transformation also introduces significant risks. Centralized health systems and interconnected IoT devices have become prime targets for hackers, jeopardizing patient data, medical equipment integrity, and ultimately, patient safety [1,2].

As health systems become more dependent on AI and electronic systems, concerns arise about the erosion of doctor-patient relationships and the prioritization of monitoring over health outcomes [3,4]. This article investigates the vulnerabilities of centralized medical technologies, presenting case studies of cyberattacks and IoT breaches, and discussing whether these systems enhance or hinder health care delivery.

Methodology

This analysis synthesizes data from peer-reviewed studies, governmental reports, and industry sources to examine the risks and impacts of centralized health care systems and IoT vulnerabilities. Key case studies and security assessments are reviewed to provide a robust understanding of the cybersecurity challenges facing modern health care [5,6].

Discussion

Centralized electronic systems: vulnerabilities and risks

Centralized health systems aim to streamline data sharing and improve efficiency, yet they introduce unique vulnerabilities:

Figure 1: "Hackable Health Care," highlighting vulnerabilities in healthcare IoT systems. It showcases connected devices such as wearable monitors, CT/MRI machines, and hospital networks under threat from cyberattacks. Visual elements include symbols of cybersecurity risks, such as broken padlocks, warning signs, and data breaches, contrasted with protective elements like shields and encryption icons.

- Cyberattacks on IoT Devices
- In 2019, IoT cyberattacks increased by 300%, with hospitals and clinics being primary targets [7].
- Researchers demonstrated the ability to manipulate CT and MRI images using a small computing device, showcasing the potential for malicious interference with diagnostic tools [8].
- Erosion of Doctor-Patient Relationships
- Reliance on centralized systems often prioritizes data collection and monitoring over direct patient care [9,10].
- Patients may feel alienated as medical professionals focus more on technology than personal interactions.
- Financial and Privacy Costs
- Cyberattacks on IoT devices lead to significant financial losses and HIPAA violations. For example, the theft of an unencrypted laptop resulted in a $1.55 million fine for HIPAA non-compliance [11,12].
- Breaches of wearable device data, such as the MyFitnessPal hack in 2018, compromised sensitive health information of millions of users [13,14].

IoT device vulnerabilities

The rapid adoption of IoT devices has revolutionized health care but created new cybersecurity challenges:

- **SweynTooth Vulnerabilities**
  - Exploits in Bluetooth Low Energy (BLE) technology have been identified in 480 devices, including medical wearables and monitors [15,16].
  - These vulnerabilities allow hackers to manipulate medical data and potentially harm patients.
- **Wearable Technology Risks**
  - Devices such as fitness trackers and biosensors are increasingly used for health monitoring, yet they remain susceptible to data breaches and hacking [17,18].
  - Examples include hackers controlling Modius Headbands to alter electrical currents, causing physical discomfort [19].
- **Systemic Threats**
  - Centralized IoT architectures create single points of failure, making entire systems vulnerable to coordinated attacks [20,21].

Solutions

Enhancing cybersecurity protocols

- **Implement Zero-Trust Security Models:** Ensure that all data and devices are authenticated and authorized at every stage of communication [22,23].
- **Regular Software Updates:** Consistently update software and firmware on IoT devices to mitigate newly discovered vulnerabilities [24,25].

Decentralizing systems

- Reduce reliance on centralized health systems by employing network segmentation to isolate critical systems from non-essential ones [26,27].

- Use decentralized data storage systems to minimize the impact of breaches on patient data [28,29].

Strengthening regulations

- Enforce stricter penalties for non-compliance with HIPAA and cybersecurity standards [11,12].
- Mandate encryption for all medical data storage and transmission [10,13].

Detoxification to deactivate connections to the internet of brains and internet of things

As IoT systems grow increasingly pervasive, exposure to harmful electromagnetic fields (EMFs) and digital monitoring technologies becomes a concern. Incorporating MasterPeace Zeolite Z™ and SOLergy Sea Minerals™ into a detoxification strategy can mitigate these effects:

- MasterPeace Zeolite Z™
- **Action:** Binds to heavy metals, nanomaterials, and synthetic chemicals, including those potentially used in IoT-connected devices.
- **Benefits:** Helps deactivate harmful nanoparticles and nanobots that may connect individuals to IoT networks or AI-driven systems like the Internet of Brains [8,9,30].
- **Pathways:** Facilitates removal through respiration, urination, perspiration, defecation, and menstruation [27,30].
- SOLergy Sea Minerals™
- **Action:** Provides bioavailable trace minerals to restore the body's bioelectric integrity disrupted by IoT systems and EMFs.
- **Benefits:** Neutralizes harmful electromagnetic frequencies and supports cellular recovery, aiding in disconnection from IoT systems [9,30].
- Patient-Centered Care Models
- Invest in human-centric care that prioritizes the doctor-patient relationship over technology-driven interactions [9,28].
- Use IoT devices as tools for monitoring without undermining personal patient engagement and clinical decision-making.

Conclusion

While centralized health care systems and IoT devices offer many benefits, they also create significant vulnerabilities. Cybersecurity breaches and data manipulation have demonstrated the risks of prioritizing technology over patient care. Incorporating detoxification solutions like MasterPeace Zeolite Z™ and SOLergy Sea Minerals™, alongside robust cybersecurity protocols, decentralized systems, and patient-centered care models, ensures that technology serves as an ally, not a liability [8,9,30].

Bibliography

1. U.S. Department of Health and Human Services. "Internet of Things Security Analyst Note". (2019).
2. Fortinet. "Eavesdropping Risks in IoT". (2019).
3. Katrenko A and Semeniak E. "Internet of Things Security: Challenges and Best Practices". (2012).
4. TrendMicro. "IoT Security Issues, Threats, and Defenses". (2019).
5. Newton P. "Simplify Zero-Trust Implementation for IoT Security". (2022).
6. Kerravala Z. "How Network Segmentation Provides a Path to IoT Security". (2015).
7. MongoDB. "What is IoT Architecture?". (2021).
8. Ranger S. "What is the Internet of Things?" (2020).
9. Williams A. "Stolen Laptop Triggers $1.55 Million Fine for HIPAA Violation". (2016).
10. Monica K. "Potentially Unencrypted Laptop Stolen from LA Hospital". (2017).
11. HHS. "Mitigating Attacks Against Uninterruptible Power Supply Devices". (2020).
12. Statista. "Wearable Worldwide Statistics". (2021).
13. HHS. "Intelligence Briefing: Wearable Device Security". (2020).

14. Fortinet. “Physical Security Convergence with Cybersecurity in Healthcare”. (2019).

15. Socradar. “Common IoT Attacks That Compromise Security”. (2022).

16. SweynTooth Vulnerability Report. “Unleashing Mayhem over Bluetooth Low Energy”. (2020).

17. EideBailly. “Security Risks of Wearable Devices”. (2018).

18. CSO Online. “Security Concerns for Wearables”. (2018).

19. VPN Mentor. “Security and Privacy Flaws in Popular Wearable Devices”. (2020).

20. Fortune. “Hacked MyFitnessPal Data for Sale on the Dark Web”. (2019).

21. “Wearable Healthcare Tech Report”. (2018).

22. Eide Bailly. “Electronic Pickpocket: Security Risks of Wearable Devices”. (2018).

23. CSO Online. “8 Security Threats Wearables Pose to Companies and Individuals”. (2018).

24. Asset Group. “SweynTooth: Unleashing Mayhem over Bluetooth Low Energy”. (2020).

25. Security News. “Apple Watch Vulnerability Allows Spying on iPhone Users”. (2019).

26. Fortinet. “Securing Connected Hospitals: A Research on Exposed Medical Systems”. (2019).

27. Semantics Scholar. “Assessment of Security Vulnerabilities in Wearable Devices”. (2016).

28. Ke Wan Ching., *et al*. “Wearable Technology Devices Security and Privacy Vulnerability Analysis”. *International Journal of Network Security and Its Applications* 8.3 (2016): 19-30.

29. Fortune. “MyFitnessPal Data Breach”. (2019).

30. “HHS 405d Program Health Industry Cybersecurity Practices”. (2020).

Appendices

Appendix A: Case Studies in IoT and Health Care Security

- CT/MRI Manipulation via Raspberry Pi (2019): Israeli researchers manipulated CT and MRI data using a Raspberry Pi device, illustrating the ease of hacking sensitive medical equipment.
- SweynTooth Exploits in Wearables (2020): Vulnerabilities in Bluetooth Low Energy (BLE) enabled hackers to bypass security in 480 distinct medical devices, including blood glucose meters and biosensors.

Appendix B: IoT Device Recommendations

- Use encrypted communication protocols.
- Apply network segmentation to reduce access points for hackers.
- Employ regular firmware updates and Zero-Trust models for maximum security.