International Journal of Healthcare Management

ISSN: 2047-9700 (Print) 2047-9719 (Online) Journal homepage: www.tandfonline.com/journals/yjhm20

Securing remote patient care: Addressing cyber threats in medical devices and the cost of breaches in the US healthcare system

Yoshiyasu Takefuji

To cite this article: Yoshiyasu Takefuji (26 Aug 2025): Securing remote patient care: Addressing cyber threats in medical devices and the cost of breaches in the US healthcare system, International Journal of Healthcare Management, DOI: 10.1080/20479700.2025.2546530

To link to this article: https://doi.org/10.1080/20479700.2025.2546530

Published online: 26 Aug 2025.

INTERNATIONAL JOURNAL OF HEALTHCARE MANAGEMENT
https://doi.org/10.1080/20479700.2025.2546530

Taylor & Francis
Taylor & Francis Group

NEWS

Securing remote patient care: Addressing cyber threats in medical devices and the cost of breaches in the US healthcare system

Yoshiyasu Takefuji

Faculty of Data Science, Musashino University, Tokyo, Japan

ABSTRACT

This paper examines the security challenges in remote patient care, focusing on the vulnerabilities of medical devices to cyber threats. A thorough literature review reveals significant risks due to devices that are not FDA-regulated, leading to potential unauthorized access and cyber breaches. The findings underscore the gravity of security breaches, which cost the US healthcare system up to $6.2 billion annually, with 90% of hospitals experiencing data breaches, averaging $3.7 million in losses per incident. The paper concludes by emphasizing the necessity of safeguarding medical devices against security breaches. It offers essential advice for healthcare professionals to manage these risks effectively, which is vital for protecting patient data, maintaining trust in the healthcare system, and ensuring the financial stability of medical institutions. The integrity of remote healthcare management hinges on addressing these security concerns. To enhance the security of remote patient monitoring devices, effective collaboration among healthcare providers, manufacturers, and cybersecurity teams is essential to ensure proper authentication and protection against cyber threats and security breaches.

ARTICLE HISTORY
Received 11 September 2024
Accepted 6 August 2025

KEYWORDS
Security breach; security vulnerability; remote patient monitoring; unprotected medical device; FDA

1. Introduction

In the healthcare industry, patients are considered customers. However, managing healthcare remotely can pose risks to patients due to insecure devices and management practices and produce the extra cost for hospitals through security breaches. This paper discusses, from a value inquiry perspective, the immediate need to address this issue for healthcare education and practices. By reducing the risks of security breaches, this paper's contributions extend not only to remote patients but also to the healthcare industry. It is essential for healthcare professionals to be well-informed about the current issues concerning medical devices used for remote patients, as this knowledge is key to preventing potential economic losses. In other words, security breaches in the US have an annual cost of as much as $6.2 billion [1]. Almost 90% of hospitals have experienced data breaches [2], which on average cost each institution $3.7 million [3]. This paper explores the security concerns related to remote patients and offers advice for healthcare professionals on how to manage medical devices that are susceptible to security breaches.

A comprehensive literature review was conducted on medical device safety. William J. Gordon et al. emphasize that software plays an important role in the safety and security of medical devices [4]. This is because 'software has become an increasingly important component of medical devices' [4]. In addition to software issues of medical devices, communications of Internet-connected medical devices with Bluetooth hardware have increased security issues. There are two types of medical devices: a device with Bluetooth or Wi-Fi networking, a device with Internet-SIM (Subscriber Identity Module) embedded. SIM-based medical devices are more expensive than Bluetooth or Wi-Fi devices. SIM-based medical devices are more secure than Bluetooth or Wi-Fi devices, but for economic reasons, Bluetooth devices are more common in medical devices.

Scott Mace summarized the reasons why medical devices have security issues from three perspectives [5]:

1) Efforts to ensure the safety of Internet-connected medical devices are costly and may still be inadequate.
2) Knowledge workers in healthcare organizations cannot be expected to become security experts. 3) Economic

CONTACT Yoshiyasu Takefuji takefuji@keio.jp Faculty of Data Science, Musashino University, 3-3-3 Ariake Koto-ku, Tokyo 135-8181, Japan

> pressures on medical device vendors are driving the need for upstream security in the medical device supply chain on cloud-based systems. [5]

Updating the security of Internet of Things (IoT) devices is widely recognized as an expensive and generally ineffective process [5]. For example, when a new software flaw is discovered in a medical device – just as in any other type of software – a corresponding Common Vulnerabilities and Exposures (CVE) entry is released. This unique identifier for a specific vulnerability is published by the US-based MITRE Corporation and is employed globally by security researchers. Currently, there are 211,890 distinct CVEs, with more than 2500 new entries appearing each month. However, it is clear that not every one of these vulnerabilities is pertinent to the medical field [5].

Recent studies have linked cybersecurity breaches in hospitals to insufficient staff awareness of cybersecurity risks [6]. For example, a prominent Italian hospital with over 6000 healthcare professionals conducted an annual phishing simulation as part of its training and risk assessment initiatives [7]. Results revealed that customized phishing emails were far more likely to engage staff: 64% ignored generic emails versus only 38% bypassing customized ones, with higher click rates for the latter. However, internal issues disrupted the campaigns' execution as planned [7]. Meanwhile, the evolution of the IoT has introduced critical cybersecurity challenges [8]. IoT devices and cloud-based services, which handle sensitive information, are increasingly vulnerable to attacks. The integration of traditional and cloud systems – lacking uniform regulations – necessitates robust strategies to secure data integrity and privacy, underscoring significant IoT risks and the need for proactive solutions.

Gerke et al. addressed the need for regulation of home monitoring technologies at COVID-19 [9]. 'In the event of a COVID-19 pandemic, there is growing interest in the use of home monitoring technologies to reduce the risk of human contact and consequent exposure to the coronavirus SARS-CoV-2' [9].

The US Food and Drug Administration (FDA) considers some apps to be medium-risk devices that require 'special controls to provide reasonable assurance of safety and effectiveness and has classified this software as a medical device as a Class II device' [9], but some home monitoring technologies are not considered medical devices, thus they are not subject to FDA regulation. This means that patients using vulnerable medical devices are currently unprotected.

Patel et al. clearly stated that 'considerations of cybersecurity and data rights are preconditions for the mass adoption of Digital therapeutics defined by the Digital Therapeutics Alliance' [10]. This paper shows that the preconditions for medical devices of remote patients are never met. The editorial depicted that 'the safety and performance of medical devices should be validated in conditions and environments that are most beneficial to patients' [11]. William J. Gordon and his colleagues have proposed smartphone-based health apps for clinical practice [12], but the security issue is not resolved at all. Because the medical devices themselves have security vulnerabilities regardless of robust smartphone-based apps.

Remote patient information is sensitive and valuable, and is thus highly vulnerable to attack by cybercriminals [13]. 'A study by IBM and the Ponemon Institute reported that cyber breaches in the US cost up to $6.2 billion per year and that almost 90% of hospitals have reported a data breach' [14]. In other words, hospital data breaches cost an average of $3.7 million per organization. This is due to the rampant hacking of medical records for profit in the United States [2]. McGraw et al. conducted a literature review on cyberattack analysis and the results showed the immediate need of privacy protections to encourage use of health-relevant digital data in a learning health system [15]. Wani et al. investigated hospital bring-your-own-device (BYOD) security with smart phones of remote patients and concluded that the results suggest that all three aspects of the security process (people, policy, and technology) need equal emphasis in order to optimize BYOD security management in hospitals [16]. In other words, hospital BYOD security management requires a security review and update regarding people, policies, and technology to identify security challenges.

Medical device cybersecurity should be among the top concerns for healthcare organizations. However, remote patients are currently unprotected, and medical institutions are either unaware of or neglectful of medical device security issues.

In this paper, we summarized security issues in medical devices for remote patient monitoring. This paper also presents a solution to security vulnerability issues in medical devices to avoid security breaches.

2. Rationale

A literature review was conducted on remote patient monitoring from a security perspective. Mecklai et al. presented problems of remote patient monitoring (RPM) [17]. Rules or regulations, evaluations, and costs were discussed on RPM, but data security was rarely mentioned [17]. They described security measures only as supporting the decision to adopt a technology, but as this paper points out, they should be treated as essential.

To ensure that remote patients are not left unprotected, security needs to be taken care of. We must avoid a security breach in medical devices. The security breach is any event that leads to unauthorized access to computer data, applications, networks, or devices. This results in information being accessed without authorization.

The following are some of the causes of information leaks in healthcare-related organizations:

- Personal medical information is of high informational value because it includes personal identification information, health status, and financial status.
- Healthcare-related organizations are currently in a period of drastic changes in their business operations due to information technology, and are unable to take sufficient information security measures.
- Chronic shortage of engineers in information system management departments. In particular, there is a shortage of cybersecurity experts in healthcare-related organizations, which require complex and highly specialized skills.

Statistics of information incidents in which medical-related organizations were the source of the leak. Due to the high value of medical information, there are many information security incidents in which medical institutions are the source of the leak. According to the HIPAA Journal website, almost 40 million medical records were exposed across the USA in 2021 [18].

NIST proposed standards to secure RPM systems, emphasizing the need for strong security measures [23]. Meanwhile, Bracciale et al. analyzed cybersecurity vulnerabilities in medical devices, revealing key risk factors [5]. Singh et al. offered cloud-based IoT security strategies specifically for RPM systems to enhance device protection and data integrity [9]. Additionally, Svandova et al. reviewed existing security frameworks for medical IoT, highlighting their effectiveness and areas for improvement [24]. Together, these contributions underscore the critical importance of robust security for RPM technology.

A security vulnerability in Bluetooth components was recently disclosed including many connected medical devices through PCs or smart phones [19]. 'Besides, the hundreds of millions of devices already in the field can't be patched to eliminate this vulnerability' [19].

Hackers or malicious groups are targeting smart phones through Bluetooth devices [20]. For examples, Bluesmack is a cyber-attack done on Bluetooth-enabled medical devices [21]. Basically, it is the type of DoS attack for Bluetooth which disables Bluetooth communications [21]. Bluesmack could suddenly interfere with the use of RPM and in doing so put patients at risk, such as not being able to detect worsening medical conditions. Even if the data is breached through networked medical devices, it has to be encrypted so that the breached data cannot be easily seen by malicious hackers.

Medical doctors/engineers and patients must be aware of vulnerabilities of medical devices.

Although there are many studies of excellent monitoring technologies, there is a lack of consideration of security aspects [22]. When RPM being expanded without being fully validated and with suppressed medical costs, it can be assumed that there will not be enough resources for security measures. This paper aims to serve as a stepping stone to reflect security measures for RPM systems in cost estimation. The guidelines published by NIST (SP 1800-30, 2021) 'notes the application of people, process, and technology as necessary to implement a holistic risk mitigation strategy' [23]. These guidelines will help doctors and technicians to make RPM safer.

Managing hospital Bring-Your-Own Device (BYOD) security for remote patient smartphones means reviewing and updating all three aspects of the security process: people, policy, and technology. 'This requires identifying the key security challenges associated with hospital BYOD use and providing additional practical insights from current BYOD practices' [16].

3. Discussions

Remote patient monitoring (RPM) has emerged as a valuable tool for healthcare, offering improved care accessibility and management. However, this progress is critically threatened by a significant vulnerability: the lack of robust security in medical devices used for RPM [5,8,23,24]. This discussion delves into the security risks associated with RPM and proposes solutions to address this pressing issue.

The inherent risk lies in the devices themselves [5]. Many rely on Bluetooth or Wi-Fi connections, which are susceptible to hacking, thereby creating a gateway for malicious actors to access sensitive patient data. This could potentially compromise diagnoses, treatment plans, and even personal identification information. The consequences can be dire, jeopardizing patient safety and exposing individuals to identity theft.

Economic considerations further complicate the issue. Implementing robust security measures can be costly, leading healthcare providers to prioritize cost-cutting over security. However, this approach proves to be a false economy; data breaches can incur significant financial penalties, not to mention the reputational damage and potential lawsuits [1–3].

Additionally, updating the security of IoT devices is widely recognized as an expensive and generally ineffective process. When a new software flaw is discovered in a medical device, a corresponding CVE entry is released. This unique identifier for a specific vulnerability is published by the US-based MITRE Corporation, with 211,890 distinct CVEs currently existing and over 2500 new entries appearing each month [5]. Not all of these vulnerabilities, however, are relevant to the medical field.

Beyond economic concerns, a lack of awareness can exacerbate the problem. Healthcare professionals may not be fully informed about the security vulnerabilities associated with these devices. This knowledge gap hinders their ability to make informed decisions regarding device selection and patient education. Furthermore, some home monitoring technologies remain unregulated [23], creating an environment ripe for exploitation.

Compounding these vulnerabilities, recent studies have linked cybersecurity breaches in hospitals to insufficient staff awareness of cybersecurity risks. A prominent Italian hospital with over 6000 healthcare professionals conducted an annual phishing simulation as part of its training and risk assessment initiatives [7]. The results revealed that customized phishing emails significantly engaged staff; 64% of employees did not engage with generic emails, while only 38% ignored customized versions. Such findings highlight the need for continuous training and the implementation of strategic solutions.

The time to act is now. As RPM adoption continues to grow, addressing security concerns is no longer optional. This paper proposes a multi-pronged approach to create a more secure RPM environment:

1. Comprehensive Security Reviews: Hospitals and healthcare providers need to prioritize thorough security reviews of all RPM devices. These evaluations should extend beyond technology to encompass personnel and policies. Identifying vulnerabilities in training protocols and access control measures is essential alongside assessing the technical security of the devices. Regular audits and assessments can help ensure that any security gaps are promptly addressed.
2. Education and Training: Ongoing training for healthcare professionals concerning the security risks associated with RPM devices is critical. Training programs should be designed to raise awareness about the importance of security, how to recognize potential threats, and best practices for using these technologies safely. This empowerment enables healthcare professionals to select secure devices, implement proper safeguards, and educate patients on safe practices when using these technologies. Training should also include simulated scenarios that prepare staff to respond effectively to security incidents.
3. Standardized Regulations: Regulatory bodies must play a vital role in establishing clear and enforceable security standards for all RPM devices. Such standards should encompass data encryption, secure communication protocols, and device vulnerability management practices. Furthermore, the adoption of standardized security frameworks can help ensure a uniform approach to security across different devices and platforms, making it easier for healthcare providers to implement necessary controls.
4. Collaboration: Effective security solutions require collaboration between healthcare providers, device manufacturers, and cybersecurity experts. This synergy fosters the development and implementation of robust security measures tailored to the specific needs of RPM systems. Collaborative efforts could

also lead to the creation of industry-wide best practices and shared resources for addressing emerging cybersecurity threats. Joint initiatives can encourage information sharing about vulnerabilities and threats, enabling stakeholders to respond more effectively.

By prioritizing security in remote patient monitoring, we can ensure that this valuable healthcare tool reaches its full potential. Patients will benefit from improved care and management, while healthcare providers can deliver services efficiently and securely. Ultimately, collaborative action can lead to a more secure and cost-effective healthcare system for all.

Internet connectivity is typically defined as an IP-accessible network, yet the manuscript only examines mobile networks employing SIM cards, Wi-Fi (IEEE 802.11 series), and Bluetooth (IEEE 802.15 series) as examples of Layer 1 and Layer 2 connections in the OSI model. In practice, however, internet connectivity for medical devices involves a much wider range of communication methods, including wired LAN (IEEE 802.3 series) and CAN-BUS among others. Moreover, even within wireless technologies, the degree of security can vary significantly based on the encryption protocols in use. Ignoring these differences compromises the overall accuracy of the argument concerning cybersecurity. Given the inherent vulnerabilities associated with Bluetooth and Wi-Fi, it is imperative to establish stringent security protocols specifically tailored to medical devices [5,8,23,24].

Although this paper offers thorough security reviews and educational resources, healthcare organizations still require specific guidelines to effectively implement solution strategies. To improve security in remote patient monitoring, healthcare providers should conduct detailed assessments of devices, prioritize continuous education for staff regarding cybersecurity risks, establish standardized regulations for device security, and encourage collaboration among stakeholders. These strategies will promote informed decision-making, strengthen protective measures, and create a cohesive approach to tackling emerging cybersecurity challenges.

To provide a broader context, it is important to recognize that various industries beyond healthcare are grappling with similar cybersecurity challenges. For instance, the finance and energy sectors have also faced significant threats from cyberattacks, leading to substantial investments in advanced security measures and employee training programs. These industries have adopted robust regulatory frameworks, emphasizing data encryption and incident response protocols, which serve as valuable models for healthcare organizations. Learning from their experiences can inform the development of comprehensive cybersecurity strategies within healthcare, ensuring the protection of sensitive patient data while navigating the complex landscape of remote monitoring technologies.

While successful cybersecurity implementations are essential across various sectors in healthcare, we often struggle to present these examples due to the fact that past successful cases have been compromised by cyberattacks. Moreover, our current theoretical frameworks for security – especially those pertaining to individual identification – remain underdeveloped, as reflected by our enduring reliance on traditional methods like usernames and passwords over many years.

All peer-reviewed references were gathered using advanced Google search commands. These commands included key phrase operators, date constraints (using 'before' and 'after' operators), logical operators (AND/OR/exclusion), and site-specific filters such as 'site:nih.gov' from the National Library of Medicine.

4. Implications

Healthcare organizations must understand the described medical device vulnerabilities in this paper. They need the immediate actions for protecting remote patients against security breaches. As long as remote patients are not protected by vulnerable medical devices and healthcare providers are left with the issue of medical device security vulnerabilities, we must understand that preconditions for the mass adoption of Digital therapeutics are not met. In other words, under or after the pandemic we must use remote patient monitoring so that the security issues must be fixed as soon as possible.

We need the special cautions to unprotected medical devices where they are not subject to FDA regulation. Safety and cost of medical devices should be considered for adopting Digital therapeutics.

5. Conclusion

Although many Digital therapeutics papers emphasize safety of medical devices, the current preconditions are not met at all for adopting Digital therapeutics. Security must be considered for protecting remote patients against security breaches. An easy solution might be based on encryption of medical data on medical devices. Healthcare organizations must understand and be aware of the security vulnerabilities of medical devices. We need the special cautions to unprotected medical devices where they are not subject to FDA regulation. If the goal of cybersecurity is to protect data, networks, and devices from cyber threats and ensure a secure, risk-free environment, then we have failed in remote patient monitoring. Unless any action is taken against the vulnerability of remote patients, many remote patients will suffer security breaches that cost an average of $3.7 million per organization.

5.1. Implications for practice, policy, and/or research

The hundreds of millions of medical devices have security vulnerability. Cyber breaches in the US cost up to $6.2 billion per year with 90% of hospitals. There are many unprotected medical devices that are not regulated by the FDA. Medical device security breaches have been neglected by healthcare organizations. Security must be reconsidered and cared for remote patient monitoring.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Contributors: Yoshiyasu Takefuji completed this research and wrote this article.

Ethical approval: Not applicable.

Data availability statement

This research has no associated data.

Notes on contributor

Yoshiyasu Takefuji holds impressive global rankings in various fields of computer science, with a notable 54th place out of 395,884 in neural networks (AI), 23rd out of 47,799 in parallel computing, and an outstanding 14th out of 7,222 in parallel algorithms.

ORCID

Yoshiyasu Takefuji http://orcid.org/0000-0002-1826-742X

References

[1] Hossain MM, Hong YA. Trends and characteristics of protected health information breaches in the United States. AMIA Annu Symp Proc. 2020;2019:1081–1090.
[2] Ghafur S, Kristensen S, Honeyford K, et al. A retrospective impact analysis of the WannaCry cyberattack on the NHS. NPJ Digit Med. 2019;2:98. doi:10.1038/s41746-019-0161-6
[3] Wei Q, Pan S, Liu X, et al. The integration of AI in nursing: addressing current applications, challenges, and future directions. Front Med. 2025;12:1545420. doi:10.3389/fmed.2025.1545420
[4] Gordon WJ, Stern AD. Challenges and opportunities in software-driven medical devices. Nat Biomed Eng. 2019;3:493–497. doi:10.1038/s41551-019-0426-z
[5] Bracciale L, Loreti P, Bianchi G. Cybersecurity vulnerability analysis of medical devices purchased by national health services. Sci Rep. 2023;13(1):19509. doi:10.1038/s41598-023-45927-1
[6] Gioulekas F, Stamatiadis E, Tzikas A, et al. A cybersecurity culture survey targeting healthcare critical infrastructures. Healthcare. 2022;10(2):327. doi:10.3390/healthcare10020327
[7] Rizzoni F, Magalini S, Casaroli A, et al. Phishing simulation exercise in a large hospital: a case study. Digit Health. 2022;8:20552076221081716. doi:10.1177/20552076221081716

[8] Singh N, Buyya R, Kim H. Securing cloud-based internet of things: challenges and mitigations. Sensors. 2024;25(1):79. doi:10.3390/s25010079
[9] Gerke S, Shachar C, Chai PR, et al. Regulatory, safety, and privacy concerns of home monitoring technologies during COVID-19. Nat Med. 2020;26:1176–1182. doi:10.1038/s41591-020-0994-1
[10] Patel NA, Butte AJ. Characteristics and challenges of the clinical pipeline of digital therapeutics. NPJ Digit Med. 2020;3:159. doi:10.1038/s41746-020-00370-8
[11] Lottes AE, Cavanaugh KJ, Chan YY, et al. Navigating the regulatory pathway for medical devices – a conversation with the FDA, clinicians, researchers, and industry experts. J Cardiovasc Transl Res. 2022;15(5):927–943. doi:10.1007/s12265-022-10232-1
[12] Gordon WJ, Landman A, Zhang H, et al. Beyond validation: getting health apps into clinical practice. NPJ Digit Med. 2020;3:14. doi:10.1038/s41746-019-0212-z
[13] Lewis N, Connelly Y, Henkin G, et al. Factors influencing the adoption of advanced cryptographic techniques for data protection of patient medical records. Health Inform Res. 2022;28(2):132–142. doi:10.4258/hir.2022.28.2.132
[14] Perakslis ED, Knechtle SJ, McCourt B, et al. Doing it right: caring for and protecting patient information for US organ donors and transplant recipients. Patterns. 2023;4(4):100734. doi:10.1016/j.patter.2023.100734
[15] McGraw D, Mandl KD. Privacy protections to encourage use of health-relevant digital data in a learning health system. NPJ Digit Med. 2021;4(1):2. doi:10.1038/s41746-020-00362-8
[16] Wani TA, Mendoza A, Gray K. Hospital bring-your-own-device security challenges and solutions: systematic review of gray literature. JMIR Mhealth Uhealth. 2020;8(6):e18175. doi:10.2196/18175
[17] Mecklai K, Smith N, Stern AD, et al. Remote patient monitoring – overdue or overused? N Engl J Med. 2021;384(15):1384–1386. doi:10.1056/NEJMp2033275
[18] Alder S. May 2021 healthcare data breach report. Available from: https://www.hipaajournal.com/may-2021-healthcare-data-breach-report/
[19] Lesniewski-Laas N. Nordic's new bluetooth security vulnerability. Available from: https://www.sunriselabs.com/News-Resources/Blog/Nordic%E2%80%99s-New-Bluetooth-Security-Vulnerability
[20] Pandas. How hackers are targeting your phone through Bluetooth. Available from: https://www.pandasecurity.com/en/mediacenter/mobile-news/hackers-targeting-bluetooth/
[21] Cybervie. BlueSmack attack | what is Bluetooth hacking? Available from: https://www.cybervie.com/blog/bluesmack-attack/
[22] Malasinghe LP, Ramzan N, Dahal K. Remote patient monitoring: a comprehensive study. J Ambient Intell Human Comput. 2019;10:57–76. doi:10.1007/s12652-017-0598-x
[23] NIST. SP 1800-30 NIST securing telehealth remote patient monitoring ecosystem (2nd draft). Available from: https://www.nccoe.nist.gov/projects/use-cases/health-it/telehealth
[24] Svandova K, Smutny Z. Internet of medical things security frameworks for risk assessment and management: a scoping review. J Multidiscip Healthc. 2024;17:2281–2301. doi:10.2147/JMDH.S459987