ACHSM Asia-Pacific Journal of Health Management

ANALYSIS OF MANAGEMENT PRACTICE

SAFEGUARDING PATIENT INFORMATION AS AN ISSUE FACED BY NURSES: A POLICY BRIEF

*Alireza Nikbakht Nasrabadi[1], Narges Norouzkhani[2], Arpi Manookian[1], Mohammad Ali Cheraghi[3], Mohsen Mohammadi[4], Zohreh Izadidastenaei[5], Amir Hossein Goudarzian[*5]*

1. Department of Medical-Surgical Nursing and Basic Sciences, School of Nursing & Midwifery, Tehran University of Medical Sciences, Tehran, Iran
2. Department of Medical Informatics, faculty of medicine, Mashhad University of Medical Sciences, Mashhad, Iran
3. Department of Nursing Management, School of Nursing & Midwifery, Tehran University of Medical Sciences, Tehran, Iran
4. Department of Medical Surgical Nursing, School of Nursing and Midwifery, Guilan University of Medical Sciences, Rasht, Iran
5. PhD Candidate of Nursing, School of Nursing & Midwifery, Tehran University of Medical Sciences, Tehran, Iran

Correspondence: amir_sari@yahoo.com

ABSTRACT

In an era of advancing technology, nurses find themselves at the forefront of protecting patient information. Safeguarding patient information is a critical concern in healthcare settings due to the potential adverse effects that can result from breaches or mishandling of this data. This invasion of privacy can have profound emotional, social, and financial repercussions for patients. In this article, possible and effective approaches were provided under evolving cybersecurity threats, balancing access and privacy, human error and insider threats, education and training, interoperability and data sharing headings. Patient information security is a complex and ever-evolving challenge for nursing professionals. Nurses must remain vigilant, well-informed, and proactive in implementing cybersecurity best practices.

KEYWORDS

patient, information, nurse, policy brief

INTRODUCTION

The problem of safeguarding patient information in healthcare refers to the challenge of ensuring the confidentiality, integrity, and availability of sensitive patient data. This data encompasses personal information, medical records, treatment plans, and diagnostic results [1]. Safeguarding patient information is a critical concern in healthcare settings due to the potential adverse effects that can result from breaches or mishandling of this data [2]. Insufficient protection of patient data can lead to privacy violations, where personal and medical details become exposed without authorization. This invasion of privacy can have profound emotional, social, and financial repercussions for patients. Identity theft is another consequence [2].

Patient information often includes personal identifiers like social security numbers and addresses. When this data is inadequately safeguarded, malicious actors can use it for fraudulent activities, resulting in financial losses and personal distress for patients [3]. Legal repercussions can follow data breaches. Healthcare organizations and responsible individuals may face fines, lawsuits, and damage to their reputations [3]. These legal consequences

can be costly and damaging to the healthcare industry. Financial losses are a direct result of data breaches, as organizations must invest in investigating, mitigating, and legally defending against breaches [4].

Additionally, a loss of patient trust can impact an organization's revenue. Reputation damage is a significant concern. Healthcare providers and organizations may suffer reputational harm in the event of data breaches. This can result in a loss of patient trust and negatively affect public perceptions of the organization's commitment to patient care and data security [2]. Patients can experience emotional distress when they discover their sensitive medical information has been mishandled. This distress can manifest as anxiety, mistrust in healthcare providers, and reluctance to seek medical care [4].

Nurses play a crucial role in safeguarding patient information to ensure patient privacy and confidentiality [5]. Protecting patient information is not only a legal and ethical responsibility but also essential for maintaining trust between healthcare providers and patients [6]. But nurses face specific challenges when it comes to safeguarding patient information. With these concerns, this policy brief addresses these challenges and provide recommendations for increasing the potential of saving patient information.

CURRENT POLICIES

Current policies for safeguarding patient information may vary by region and healthcare organization, nevertheless there are numerous common approaches followed in many healthcare settings. Here are key aspects of current policies for safeguarding patient information:

1. Health Insurance Portability and Accountability Act (HIPAA) privacy rule: Adherence to the principles of the United States Federal Health Insurance Portability and Accountability Act (HIPAA) is fundamental. Policies should outline the specific measures nurses must take to ensure compliance with HIPAA regulations regarding the privacy and security of patient information [7].
2. Implementing security policies which restrict users from software installation: Disabling unnecessary services on servers and enhancing control over incoming and outgoing traffic for essential services [8].
3. Healthcare professionals specially nurses, should practice proper data and cyber security instructions; this involves maintaining strong and regularly updated passwords and staying alert to potential cyber threats like email phishing attempts. Many institutions prioritize frequent software updates as a crucial security measure [9].
4. Access to patient data is typically limited to authorized personnel, with role-based access controls in place. This means individuals can only access information relevant to their specific job responsibilities [1].
5. Patient Consent and Authorization: Policies may outline the process for obtaining patient consent for sharing information and the instances where authorization is required. This ensures that nurses are aware of the legal requirements for disclosing patient data [8].

It's important to note that data security and privacy regulations can vary by country, and healthcare organizations are often required to comply with local laws and regulations in addition to specific standards. Compliance with these policies is crucial to protect patient information and maintain trust in healthcare systems.

POLICY IMPLICATIONS AND RECOMMENDATIONS

EVOLVING CYBERSECURITY THREATS

Nurses operate in an ever-evolving landscape of cybersecurity threats. They should understand the signs of a potential ransomware attack and be prepared to respond quickly to mitigate the damage. By constantly updating their knowledge of cybersecurity best practices, nurses can play an active role in protecting patient information [6]. Phishing is a common technique used by cybercriminals to trick individuals into revealing sensitive information, such as login credentials or personal data. Phishing attempts can occur via email, text messages, or phone calls, and attackers often pose as trusted entities [10] (please see appendix).

Reporting phishing attempts promptly and following organizational protocols is crucial in preventing data breaches. While nurses are trusted professionals, the risk of insider threats (individuals within an organization) exists in any workplace. Organizations should implement stringent access controls and monitoring mechanisms to identify unusual behavior that may indicate insider threats [10]. Nurses should also be aware of the importance of reporting

any suspicious activities they observe. The proliferation of Internet of Things (IoT) devices in healthcare, such as wearable devices and remote monitoring systems, introduces new cybersecurity risks [11]. These devices are connected to networks and may transmit sensitive patient data.

However, they can also be potential entry points for attackers if not properly secured. Nurses should be aware of the security risks associated with IoT devices and ensure they follow protocols for secure connectivity and usage. Social engineering attacks target human vulnerabilities rather than technological weaknesses. These attacks exploit psychological manipulation to deceive individuals into divulging confidential information or granting unauthorized access [12]. Nurses may be targeted through tactics such as pretexting (creating false scenarios) or baiting (enticing individuals to take specific actions) [12]. Education and training on social engineering techniques can help nurses recognize and resist these tactics.

BALANCING ACCESS AND PRIVACY

Nurses face the delicate task of balancing timely access to patient information with maintaining strict privacy measures. While nurses require quick access to patient data to provide efficient care, they must also adhere to stringent access controls and confidentiality protocols. Striking the right balance involves implementing robust authentication processes and role-based access controls [13]. Nurses should have access only to the information necessary for their specific roles and responsibilities [13].

By limiting access to a need-to-know basis, healthcare organizations can reduce the risk of unauthorized access or accidental disclosure of sensitive data. Robust authentication mechanisms, such as strong passwords, two-factor authentication, or biometric authentication, can help ensure that only authorized individuals can access patient information [14]. Nurses should follow best practices for password hygiene, avoiding common pitfalls like sharing passwords or using weak and easily guessable credentials. Regularly updating passwords and promptly reporting any suspected unauthorized access can help safeguard patient data.

Education and training play a crucial role in promoting a culture of privacy and security among nurses [15]. Nurses often communicate patient information electronically through various channels, such as email, messaging platforms, or telehealth applications. It is essential to use secure and encrypted communication methods to protect patient privacy. Nurses should be trained on secure communication practices, such as avoiding transmitting patient information through unsecured channels or using encryption tools when necessary [16].

Monitoring systems can detect anomalies in data access patterns, alerting IT departments or security teams to potential breaches. Nurses should actively participate in these monitoring efforts and report any observed irregularities. Healthcare organizations should adopt a privacy-by-design approach when developing or implementing new technologies and systems [17]. This approach involves integrating privacy and security measures from the early stages of system design. Nurses can engage in conversations with patients about the use and disclosure of their information, ensuring that patients understand their rights and have control over how their data is shared [18]. This collaborative approach promotes patient autonomy and strengthens trust between patients and healthcare providers [17].

HUMAN ERROR AND INSIDER THREATS

Human error remains a significant challenge in patient information security. Nurses, like any other healthcare professionals, may inadvertently cause data breaches through accidental disclosure or mishandling of sensitive information. Comprehensive training on data protection protocols, privacy policies, and ethical use of patient information is crucial for minimizing human error and mitigating insider threats [19].

Healthcare organizations should prioritize comprehensive training programs that address data protection protocols, privacy policies, and the ethical use of patient information. By providing nurses with the necessary knowledge and skills, organizations can reduce the likelihood of human error and ensure that nurses understand the importance of safeguarding patient data [19, 20]. Encouraging a culture of incident reporting is essential in addressing human errors and identifying potential insider threats. Nurses need to be aware of the reporting mechanisms for any data breaches, privacy incidents, or suspicious activities they come across. Prompt reporting allows for timely investigation and appropriate response to mitigate the impact of incidents [12, 16]. Monitoring systems can detect anomalies in data access patterns, triggering alerts for further investigation. Creating an environment where employees are actively engaged and aware of the importance of patient information security is key to mitigating insider threats.

Regular communication and reminders about the organization's security policies, ethical guidelines, and the potential consequences of data breaches can help foster a sense of responsibility and vigilance among nurses [16]. Nursing organizations and regulatory bodies can play a role in reinforcing ethical and professional standards related to patient information security [16].

EDUCATION AND TRAINING

The rapidly evolving nature of cybersecurity threats necessitates ongoing education and training for nurses. However, nursing education programs often offer limited formal training on cybersecurity [21]. To address this challenge, healthcare organizations should prioritize comprehensive training programs for nurses. These programs should cover a range of topics, including recognizing phishing attempts, secure communication practices, password hygiene, and incident reporting. Continuous education empowers nurses with the knowledge and skills necessary to protect patient information effectively.

Nursing programs should include dedicated courses or modules that cover essential concepts, such as data protection, privacy laws, security protocols, and ethical considerations [22]. By incorporating these topics into the curriculum, nurses can develop a solid foundation in patient information security from the outset of their careers. Collaboration with industry experts, cybersecurity professionals, and information technology specialists can help ensure that the educational content remains current and aligned with the latest trends and challenges [23]. Given the rapidly evolving nature of cybersecurity threats, continuous professional development is crucial for nurses to stay informed and maintain their skills.

Healthcare organizations should support and encourage nurses to pursue additional training, attend relevant conferences or webinars, and participate in professional associations dedicated to patient information security [23, 24]. These opportunities enable nurses to expand their knowledge, network with peers, and stay updated on the latest advancements in the field. Interdisciplinary training programs that bring together different stakeholders can enhance understanding, foster effective communication, and promote teamwork in safeguarding patient data [25]. Training programs should emphasize the importance of patient privacy, ethical responsibilities, and the potential impact of data breaches on individuals and healthcare organizations [26].

INTEROPERABILITY AND DATA SHARING

Interoperability, the seamless exchange of patient information between different healthcare systems, is vital for delivering high-quality care. However, it presents challenges in terms of patient information security [27]. Nurses must ensure that data transfers occur securely, maintaining the integrity and confidentiality of patient information across various platforms and systems. Robust encryption methods, data access controls, and secure data exchange protocols are essential in overcoming these challenges [23].

The establishment and adoption of common standards and interoperability frameworks are fundamental to ensuring seamless data exchange. Standards such as Health Level Seven (HL7) and Fast Healthcare Interoperability Resources (FHIR) provide a common language for healthcare systems to communicate and exchange data [28, 29]. Nurses should be familiar with these standards and the interoperability frameworks used in their practice settings to effectively navigate data sharing processes. Adherence to data sharing policies, privacy regulations (such as HIPAA in the United States), and organizational protocols is needed.

Understanding the principles of data classification, access controls, and encryption can help nurses maintain the confidentiality and integrity of shared information [30]. Respecting patient privacy and obtaining informed consent for data sharing are critical ethical considerations, which ensure patients have control over how their information is used and shared [31]. Interoperability and data sharing facilitate access to comprehensive patient information, empowering nurses to make informed clinical decisions and collaborate with multidisciplinary care teams. Integrated electronic health record (EHR) systems enable nurses to access up-to-date patient data, including medications, allergies, and diagnostic results, supporting more efficient and coordinated care delivery [1].

Data sharing across healthcare organizations and research institutions enables advancements in medical research, population health management, and public health initiatives. Nurses may contribute to research studies or participate in data collection efforts that require the sharing of de-identified patient data. Variations in data formats, data quality, and system compatibility can hinder seamless exchange. Nurses should be prepared to address these challenges by advocating for standardized data capture, participating in data quality improvement

initiatives, and collaborating with healthcare IT professionals to enhance system interoperability [32].

CONCLUSION

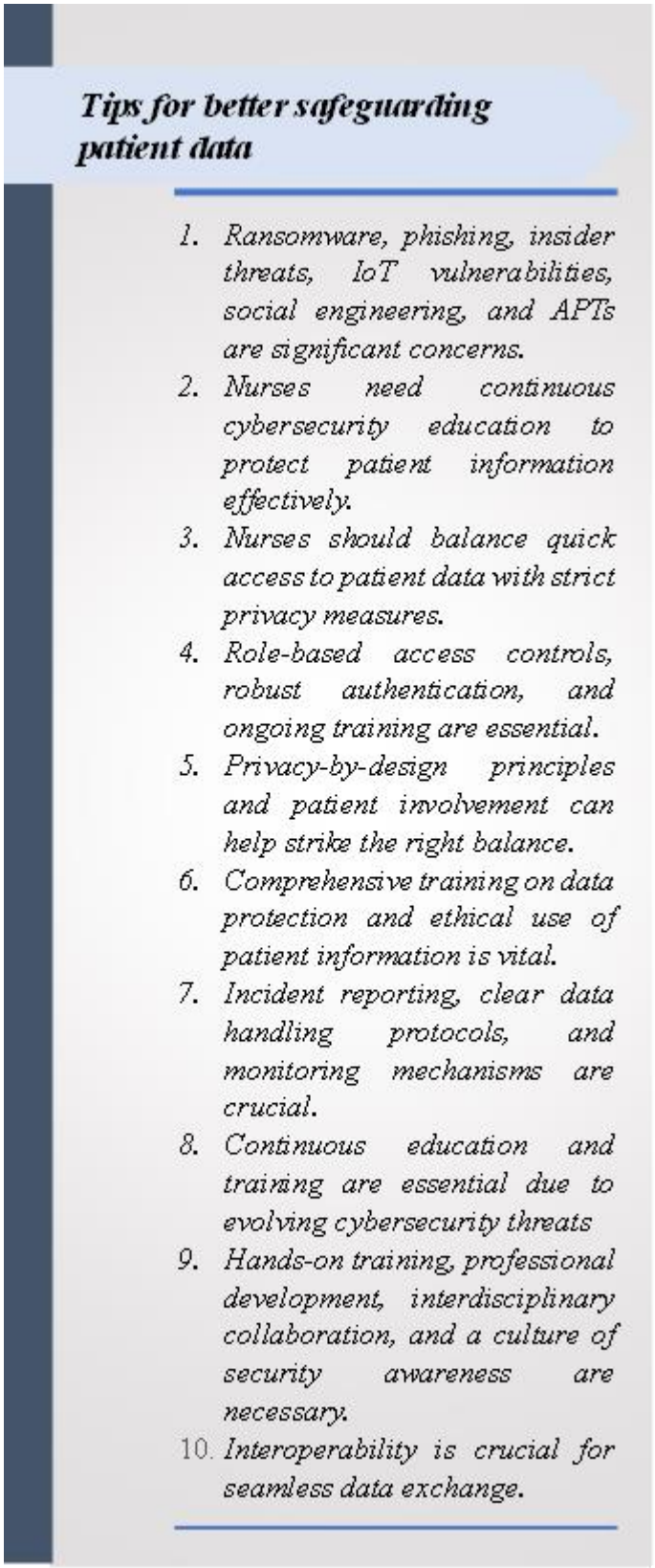
Patient information security is a complex and ever-evolving challenge for nursing professionals. Nurses must remain vigilant, well-informed, and proactive in implementing cybersecurity best practices. By addressing the evolving cybersecurity threats, balancing access and privacy, mitigating human error and insider threats, and investing in education and training, nurses can contribute significantly to safeguarding patient data. By prioritizing patient information security, nurses play a crucial role in ensuring the privacy, confidentiality, and integrity of healthcare systems in the digital age.

References

1. Keshta I, Odeh A. Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal. 2021;22(2):177-83.
2. Sokolova M, El Emam K, Rose S, Chowdhury S, Neri E, Jonker E, et al., editors. Personal health information leak prevention in heterogeneous texts. Proceedings of the workshop on adaptation of language resources and technology to new domains; 2009.
3. Kaelber DC, Bates DW. Health information exchange and patient safety. Journal of Biomedical Informatics. 2007;40(6):S40-S5.
4. Nadzam DM. Nurses' role in communication and patient safety. Journal of Nursing Care Quality. 2009;24(3):184-8.
5. Emami Zeydi A, Karkhah S. Nursing the future: How artificial intelligence empowers critical care nurses to revolutionize intensive care unit rehabilitation. J Nurs Rep Clin Pract. 2023;2(Issue 1):1-2.
6. Koivunen M, Saranto K. Nursing professionals' experiences of the facilitators and barriers to the use of telehealth applications: a systematic review of qualitative studies. Scandinavian Journal of Caring Sciences. 2018;32(1):24-44.
7. Bhate C, Ho CH, Brodell RT. Time to revisit the Health Insurance Portability and Accountability Act (HIPAA)? Accelerated telehealth adoption during the COVID-19 pandemic. Journal of the American Academy of Dermatology. 2020;83(4):e313-e4.
8. Ravi AR, Nair RR. Cybersecurity Threats and Solutions in the Current E-Healthcare Environment: A Situational Analysis. Medico-Legal Update. 2019;19(2):141-4.
9. Ronquillo JG, Erik Winterholler J, Cwikla K, Szymanski R, Levy C. Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information. JAMIA Open. 2018;1(1):15-9.
10. Rosas C. The future is femtech: Privacy and data security issues surrounding femtech applications. Hastings Business Law Journal. 2019;15:319.
11. Kumar S, Tiwari P, Zymbler M. Internet of Things is a revolutionary approach for future technology enhancement: a review. Journal of Big data. 2019;6(1):1-21.
12. Jamil F, Ahmad S, Iqbal N, Kim D-H. Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals. Sensors. 2020;20(8):2195.
13. Samadbeik M, Gorzin Z, Khoshkam M, Roudbari M. Managing the security of nursing data in the electronic health record. Acta Informatica Medica. 2015;23(1):39.
14. Nazari AM, Zare-Kaseb A, Esmaeili S. Moral courage: A suitable solution for reducing nursing error reporting. J Nurs Rep Clin Pract. 2023:1-2.
15. Li M, Lou W, Ren K. Data security and privacy in wireless body area networks. IEEE Wireless Communications. 2010;17(1):51-8.
16. Masrom M, Rahimly A. Overview of data security issues in hospital information systems. Pacific Asia Journal of the Association for Information Systems. 2015;7(4):5.
17. Forsman B, Forsgren S, Carlström ED. Nurses working with Manchester triage–The impact of experience on patient security. Australasian Emergency Nursing Journal. 2012;15(2):100-7.
18. Curtis A, Brown L, Sagong H. Nursing students' perceptions of older adults, confidence, and anxiety level changes with their first clinical rotation: A descriptive pilot study. J Nurs Rep Clin Pract. 2023:1-5.
19. Griffith R. Electronic records, confidentiality and data security: the nurse's responsibility. British Journal of Nursing. 2019;28(5):313-4.
20. Luo E, Bhuiyan MZA, Wang G, Rahman MA, Wu J, Atiquzzaman M. Privacyprotector: Privacy-protected patient data collection in IoT-based healthcare systems. IEEE Communications Magazine. 2018;56(2):163-8.
21. Kamerer JL, McDermott D. Cybersecurity: Nurses on the front line of prevention and education. Journal of Nursing Regulation. 2020;10(4):48-53.
22. Albarrak AI. Information security behavior among nurses in an academic hospital. HealthMED. 2012;6(7):2349-54.

23. Bani Issa W, Al Akour I, Ibrahim A, Almarzouqi A, Abbas S, Hisham F, et al. Privacy, confidentiality, security and patient safety concerns about electronic health records. International Nursing Review. 2020;67(2):218-30.
24. Risling T. Educating the nurses of 2025: Technology trends of the next decade. Nurse Education in Practice. 2017;22:89-92.
25. Latifi N, Roohi G, Mahmoodi-Shan GR, Tatari M. Nurses' clinical decision-making models in the care of older adults: A cross-sectional study. J Nurs Rep Clin Pract. 2023:1-6.
26. Golay D, Karlsson MS, Cajander Å. Effortlessness and Security: Nurses' Positive Experiences With Work-Related Information Technology Use. CIN: Computers, Informatics, Nursing. 2022;40(9):589-97.
27. Oliveira D, Duarte J, Abelha A, Machado J. Step towards interoperability in nursing practice. Data Analytics in Medicine: Concepts, Methodologies, Tools, and Applications: IGI Global; 2020. p. 865-78.
28. Ayaz M, Pasha MF, Alzahrani MY, Budiarto R, Stiawan D. The Fast Health Interoperability Resources (FHIR) standard: systematic literature review of implementations, applications, challenges and opportunities. JMIR Medical Informatics. 2021;9(7):e21929.
29. Quinn J. An HL7 (health level seven) overview. Journal of AHIMA. 1999;70(7):32-4; quiz 5.
30. Oyeleye OA. The HIPAA Privacy Rule, COVID-19, and nurses' privacy rights. Nursing. 2021;51(2):11-4.
31. McNett M. Protecting the data: Security and privacy. Data for Nurses: Elsevier; 2020. p. 87-99.
32. Kang J, Seomun G. Information security in nursing: A concept analysis. Advances in Nursing Science. 2021;44(1):16-30.

APPENDIX



Source: Developed by authors.