Cybersecurity: Nurses on the Front Line of Prevention and Education

Jessica L. Kamerer, EdD, MSN, RNC-NIC, and Donna McDermott, PhD, RN, CHSE

Cybercrime has become an increasing concern for consumers in the United States and internationally. In recent years, cybercrimes in the healthcare industry have drastically increased in type, impact, and frequency. These attacks have negatively impacted patient privacy, the ability of providers to deliver care, and the security of healthcare organizations. Nurses are uniquely positioned to help protect against and report cybercrimes because they are one of the largest employed populations in the healthcare industry and they are on the front line of patient care and healthcare technology use. This article discusses the main concerns of cybersecurity in healthcare, the nurse's role in preventing and managing cyber security, and recommendations for nurses, educators, and regulators.

Keywords: Continuing education, cybersecurity, electronic health records, nursing informatics, patient safety, protected health information

Cybersecurity involves protecting information by preventing, detecting, and responding to cyberattacks (Cybersecurity and Infrastructure Security Agency, 2009). Despite highly advanced technology safeguards such as audits, authentication, authorization, and data privacy measures such as encryption, human error can cause breeches in security; thus, cybersecurity remains a high priority (McDermott, Kamerer, & Birk, 2019). Mistakes among healthcare personnel, which often result from a lack of knowledge and education regarding cybersecurity safety, can be alleviated through education and proper training (Wanyonyi, Rodrigues, Abeka, & Ogara, 2017). In 2017, nurses comprised the largest percentage of healthcare workers in the nation, with more than 2.9 million nurses working in hospitals (Carlson, 2017). For this reason, nurses must be properly trained to recognize, assess, and report cybersecurity threats within their organization as part of the informatics and healthcare technologies curriculum. The widespread use of electronic health records (EHRs), healthcare information system networks, wireless and cloud information transactions, and technology-based equipment present challenges for nurses managing technology in their daily job functions. As frontline users, nurses also play a vital role in securing protected health information (PHI) and the information of multiple stakeholders, including patients, colleagues, healthcare organizations, and nurses themselves.

Background

Prevalence and Impact of Cybercrime

The prevalence of healthcare cybercrime has become increasingly widespread. Cyberattack is an international threat to patient care and safety and crosses all healthcare settings. In a study by Luna, Rhine, Myhra, Sullivan, and Kruse (2016), 94% of healthcare agencies reported internal and external cyberattacks on patient data. The security of (EHRs) and maintenance of personal health information privacy are critical priorities for all healthcare agencies (Jilka, Callahan, Sevdalis, Mayer, & Darzi, 2015). Internal cyberthreats may occur from disgruntled employees, employees who do not have proper cybersecurity training, or outside attackers, also know as hackers. Both internal and external types of cyberthreats are of concern to anyone who has access to an EHR, especially nurses who access information repeatedly during their workday and may be unaware of how their actions affect patient information safety.

The repercussions of these attacks can become a financial and personal nightmare for patients and families. In 2013, it was estimated that Americans spent $12 billion to deal with the consequences of their compromised medical files (Luna et al., 2016). Some of the consequences of compromised patient health information include theft, fraud, and abuse. Of note, a medical record number is extremely more valuable than a social security number on the black market because it carries a large amount of additional information that can also be stolen, such as social security numbers, personal information, health information, and insurance and payment details (Luna et al., 2016; McDermott et al., 2019).

In 2015, healthcare agencies were victimized more than 187 times, which compromised the personal PHI of 84 million patients (McCarthy, 2015). Cybercriminals can cripple a healthcare organization through hacking, deploying malware and ransomware, and stealing data. Compromised EHRs may cause serious harm to patients by interrupting treatment, which can potentially lead to personal harm or death. Identity theft and data tampering may also result in astronomical personal costs to patients and healthcare personnel in the form of credit fraud, legal fees, and overdraft charges, as well as the emotional toll and stress of dealing with these repercussions.

Cybersecurity in Nursing Curriculum

Given the prevalence of healthcare technology and informatics use in nursing practice, the American Association of Colleges of Nurses (AACN) recognized the need to integrate informatics curriculum into nursing degree programs. The AACN *Essentials of Master's Education in Nursing* (AACN, 2011) and the *Essentials of Baccalaureate Education for Professional Nursing Practice* (AACN, 2008) directs curricula for nursing degree programs related to informatics and healthcare technologies. These essentials recognize technology as critical to the delivery of patient care by nurses and requires programs they accredit to address these concepts in their curricula. The AACN further recognizes "that the master's-prepared nurse uses patient-care technologies to deliver and enhance care and uses communication technologies to integrate and coordinate care" (AACN, 2011, p. 5). As frontline workers, nurses are accountable for using technology effectively, safely, and efficiently. This accountability should include competency in maintaining the security of sensitive data related to patient information and the care nurses provide.

In 2012, the National Council of State Boards of Nursing (NCSBN) developed guidelines for social media use (Spector & Kappel, 2012) in recognition of the rapidly changing "user-generated" technology environment that may affect patient care and PHI. The NCSBN suggested prelicensure nurses apply concepts of information technology use to nursing practice by including it as an element in the 2016 NCLEX test blueprint in the management of care category. This category may include security plans, safe use of equipment, and reporting of incidents, errors, or variances (NCSBN, 2015). The NCSBN also recognized emerging nursing informatics issues as key elements in the transition to practice for new nurses entering the profession in a dedicated Transition for Practice module (NCSBN, n.d.). While these are important first steps in response to rapidly changing technologies used by nurses, none of the aspects of the threats to the security of EHRs have been addressed by regulatory boards. The learning objectives do not include a concept related to cybersecurity in relation to EHR, PHI, or nursing informatics.

In addition, despite the need to integrate this content into nursing degree programs, the recognition of properly educating nurses on their role in cybersecurity has faltered. The rate of healthcare security breaches rises each year, accounting for 21% of all cybersecurity breaches across the world (Heald, 2016). Quality and Safety Education for Nurses calls for nurses to meet a minimal competency in informatics to safely and effectively provide patient care. The competency relates to the nurses' involvement in the design, implementation, use, and evaluation of healthcare technology in patient care (Hunt, 2012). However, it does not quantify where maintaining security intersects with the concepts of informatics in nursing roles or education. Both novice and experienced nurses struggle with learning how to use the technology and have little knowledge about how their use of it may affect patient safety.

Aim

This article summarizes areas of cybersecurity that directly relate to the role of the nurse as well as provide recommendations for curricular inclusion of measures to prevent or respond to a cyberattack and mitigate the harm to patients and healthcare organizations. In addition, recommendations are provided for regulatory boards to suggest inclusion of cybersecurity training as continuing education (CE) for license application and renewal.

Methods: Analysis of Cybersecurity Practices in Nursing

PubMed (Medline), Cumulative Index of Nursing and Allied Health Literature (CINAHL), and ProQuest databases were used to conduct literature searches related to cybersecurity threats in healthcare and cybersecurity education in nursing programs with various inclusion and exclusion criteria. Search criteria were limited to blinded, peer-reviewed scholarly articles published in English after 2010.

Key terms used in the search were (a) electronic health record security, (b) cybersecurity in healthcare, (c) security informatics, (d) electronic medical record security, (e) nursing cybersecurity, (f) nursing education informatics, (g) nursing cyber security human factors, and (h) private health information security. The search yielded an initial sample of 70 articles. Each article was screened by the authors for threats to cybersecurity that were specific to EHR and nursing. Because little research has been conducted on this subject, we also included informational articles and position papers. Twenty-five papers were reviewed by the research team to determine the top threats to cybersecurity in healthcare and the literature-based recommendations to address or prevent cyberthreats related to nursing education and professional role. From these findings, the most common cyberthreats and recommendations for nurses to prevent or address them were identified. Next, a review was conducted of each state's board of nursing to identify states requiring CE related to informatics or cybersecurity considerations in nursing practice.

Results

Top Cyberthreats to Healthcare Identified

The growing number of security threats in healthcare, particularly against EHRs, has led to concerns regarding security of personal and financial information (Seckman, 2018). Achieving information security is an essential topic in nursing informatics (Banerjee, Rao, Tamakuwala, & Koru, 2018). However, most of the literature regarding cybersecurity related to the healthcare market is lacking nursing-specific practice considerations. The articles reviewed revealed trends and deficiencies across healthcare systems and were analyzed to identify their correlation to professional standards and practice implications for nurses. Much emphasis has been placed on using EHR systems, integrating medical records and data collection into the nursing procedures of delivering care, and managing informatics as part of the nursing role. However, outside of hospital-based education, little education exists regarding the need to protect EHR systems and PHI of patients from cyberthreats by nurses.

The U.S. Department of Health and Human Services (HHS) states that a cyberthreat is or has the potential to cause unauthorized disclosure, unavailability, changes, or destruction of an asset (HHS, 2018, 2019). Cyberthreats include the compromise of patient information, inability to access information systems vital to nursing and other providers' job functions, or destruction of system or patient information. Top areas for cybercrime within healthcare were identified and included: (a) physical threats, (b) portable devices, (c) internal users, (d) technical threats, and (e) administrative threats (McDermott et al., 2019). Although many technological safety features were available to prevent and safeguard against cyberattacks or threats, the human factor remained one of the most prevalent areas of concern in the literature, including the role of the healthcare worker, especially the nurse, in maintaining EHR safety (McDermott et al., 2019).

Physical threats occur when nonelectronic records are lost, accidentally discarded, or stolen. Actions such as leaving a workstation unsecured or improperly filing or disposing of documents may be unintentional; however, they present serious concerns regarding the safety and protection of a patient's PHI.

According to Blanke and McGrady (2016), portable device breaches were the highest number of reported threats and remained especially vulnerable to cyberattacks. Lost, stolen, or unattended devices such as cell phones, laptops, and other mobile equipment contributed to this type of cyberthreat (Namoglu & Ulgen, 2013).

Because it is difficult to control for the decisions and actions of employees, EHR internal users remain one of the weakest links in safeguarding patient PHI (Parikh, 2018). Healthcare workers who intentionally delete, change, or misuse data, as well as those who intentionally violate computer safety protocols within the organization, contribute to insider cyberattack (HHS, 2019).

Technical threats may be used to extract a patient's secure health information by tricking the user into providing passwords or other personal information (HHS, 2019). These include social engineering threats such as identity theft, ransomware, phishing, and spoofing. Phishing and spoofing refer to the creation of a fake website that appears legitimate to entice users and gain access to their personal information such as passwords.

Administrative threats are breakdowns in protocols, policies, and procedures of the daily operations of an EHR. Security policy breaches and improper staff training leave healthcare agencies open to cyberattack.

Recommendations for Nurses: Cybersecurity Prevention and Response

As EHR use has proliferated in the United States, additional education on the prevention of cyberthreats has become imperative at the hospital and in turn, arguably, the academic and regulatory levels. While nurses are not expected to understand the complicated code bases or system implementation technology aspects of cybersecurity, they are able to prevent and respond appropriately to cyberattacks as part of their role and professional responsibilities. Table 1 provides recommendations for nurses in safeguarding PHI of patients through increased cybersecurity awareness according to categories of identified threats in the literature.

Recommendations for Nursing Education: Cybersecurity Curriculum

The Technology Informatics Guiding Education Reform (TIGER) initiative was founded in 2004 to develop a shared vision and provide specific strategies for improving nursing education and practice related to the use of health information technology. TIGER makes recommendations for information literacy and management competencies. The information management competency acknowledges that due care is needed by the nurse regarding confidentiality of protected patient health information and also for EHR access control (Healthcare Information and Management Systems Society, 2010). TIGER has been a leader in driving informatics education and programs related to health information technology since its inception.

The common thread missing from previous informatics and health technology education has been the nurse's role in preventing and reporting cyberthreats and in maintaining cybersecurity. Systems of higher education that educate healthcare and IT professionals should research and consider the feasibility and best practices of providing this education, as these workers are vital in helping to stop cyberthreats and security breaches in the field (McDermott et al., 2019). The World Medical Association (2016) also recommends that undergraduate and graduate medical education curricula include comprehensive information on technology and cybersecurity measures.

Recommendations for Nursing Regulation: CE

Since 2019, 70% of state boards of nursing require CE to maintain or renew nursing licensure in the United States. Twenty-nine percent of states do not require any CE for license renewal or maintenance, and only 10% require working a set minimum number of practice hours or proving professional competency in some other form within in a renewal period to maintain licensure (AAACEUs, 2019). Twenty percent of states require specific topics of CE completion for nursing license maintenance. For example, one state requires all nurses to complete a minimum of 2 hours of CE on reporting and recognizing child abuse; however, no states require CE on informatics or cybersecurity of patient PHI to maintain licensure (AAACEUs, 2019).

TABLE 1

Cybersecurity Threats and Prevention Measures

Type of Threat	Threat Examples	Preventive Measures
Physical	***Unintentional employee actions such as improper document disposal***	***Shred or properly dispose of all hard copy documents***
	• Leaving workstations unsecured • Responding to a phishing request	• Secure documents in locked file cabinets • Sign off work station before leaving • Never share passwords • Never click on unsecured or unknown links from work stations • Notify IT of any suspicious emails
Portable Devices	***Lost or stolen device***	***Notify IT security immediately of any lost or stolen devices***
	• Unsecured data uploading to cloud-based systems	• Store portable devices in locked storage areas or charging stations • Maintain locator technology on devices and use sign out sheets • Compliance with hospital policies on use and storage of any portable devices (eg, phones, workstations, tablets, patient equipment) • Maintain encryption/decryption when uploading to the cloud • Never share portable device passwords with other users or allow others to use your device with your password
Insider Use	***Intentional violation of cybersecurity protocols through unauthorized access or deletion of data***	***Computer competency training that includes safeguarding measures***
	• Disgruntled employee deleting data	• Recognition of the legal and ethical implications of EHR use • Proper onboarding and termination procedures • Ensuring a healthy workplace culture to avoid emergence of employees • Prompt reporting of any suspicious employee actions regarding EHR use • Software intervention (eg, firewalls, encryption, access restriction) • Immediate response to breaches
Technical	***Social engineering threats that manipulate human trust (eg, identity theft, ransomware, phishing, spoofing)***	***Working with IT professionals to identify and report phishing emails***
		• Frequent password changes using high complexity strength • Updating systems as requested • Maintaining encryption and protection of devices
Administrative	***Breakdown of day-to-day operations and policies***	***Compliance with all IT security policies for safeguarding PHI***
		• Education regarding deletion or use of data • Staff training on data access and usage • Ensure that IT privileges and access match employee responsibilities

Note. EHR = electronic health record; IT = information technology; PHI = protected health information

With the proliferation of healthcare technology over the past 5 years and unknown future technological disruptors, it is crucial that nurses become educated on cybersecurity threats that may impact their practice and their patients. Given the crisis of cybersecurity threats and breaches in healthcare demonstrated in the literature, all nurses—not only new graduates—must be educated on their role in preventing and managing cybersecurity while working with PHI of patients. While academic settings are beginning to respond to the need for education regarding cybersecurity, practicing nurses may not have the same opportunities for learning. For example, acute care hospitals were the most common setting for nursing informatics research sites (Carrington, et al., 2018), but other professional areas such as school districts also reported adoption of informatics and EHR (Wilburn, 2018). Recognizing a need for CE related to cybersecurity may be one way to ensure understanding of these concepts. Regulatory boards are uniquely positioned to suggest the incorporation of cybersecurity training with suggestions for licensing examination blueprints, transition to practice modules, and nursing CE for licensure.

Conclusion

The financial and personal repercussions to patients due to breaches in PHI are significant. Healthcare organizations and employees suffer from cybersecurity threats and breaches. Because nurses play such an integral part of protecting patient PHI, healthcare technology is an integral part of their professional role. While educational programs may be one way to begin incorporating this curricular content, experienced practicing nurses may remain unaware of these important concepts related to cybercrime and cybersecurity. In addition, nurses have different levels of expertise using EHR information systems; therefore, cybersecurity is an important learning concept for all nurses. Other recommendations include incorporating material in NCLEX examinations and blueprints, Transition to Practice modules, and hospital/community orientation programs. Reaching experienced practicing nurses may be achieved through regulatory suggestions of CE on cybersecurity both at the state and national levels. Education of students and nurses on the importance of cybersecurity is critical to maintaining a safe standard of care for patients and protecting their PHI.

References

AAACEUs. (2019, July 23). *Nursing continuing education requirements by state.* Retrieved from https://www.aaaceus.com/state_nursing_requirements.asp

American Association of Colleges of Nurses. (2008, October 20). *The essentials of baccalaureate education for professional nursing practice.* Retrieved from http://www.aacnnursing.org/portals/42/publications/baccessentials08.pdf

American Association of Colleges of Nurses. (2011, March 21). *The essentials of master's education in nursing*. Retrieved from http://www.aacnnursing.org/portals/42/publications/mastersessentials11.pdf

Banerjee, U., Rao, P., Tamakuwala, P., & Koru, G. (2018). *Achieving information security in healthcare information systems: An essential challenge for the future of nursing informatics.* Presented at 28th Summer Institute in Nursing Informatics, Baltimore, MD.

Blanke, S. J., & McGrady, E. (2016). When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: A cybersecurity risk assessment checklist. *Journal of Healthcare Risk Management, 36*(1), 14–24.

Carlson, K. (2017, March 31). March 2017 release of BLS employment statistics report: First look. Retrieved from https://nurse.org/articles/march-2017-release-bls-report-first-look-nursing/

Carrington, J. M., Estrada, N., Brittain, A. C., Dudding, K. M., Galatzan, B. J., Nibbelink, C., … Renz, S. M. (2018). Nursing informatics year in review 2017. *Nursing Administration Quarterly, 42*(2), 180–185.

Cybersecurity and Infrastructure Security Agency. (2009, May 6). Security tip (ST04-001): What is cybersecurity? Retrieved from https://www.us-cert.gov/ncas/tips/ST04-001

Heald, K. (2016). Why the insurance industry cannot protect against health care data breaches. *Journal of Health Care Law and Policy, 19*(2), 275–292.

Healthcare Information and Management Systems Society. (2010). The TIGER Initiative Informatics Competencies for Every Practicing Nurse: Recommendations from the TIGER Collaborative. Retrieved from http://www.thetigerinitiative.org/

Hunt, D. (2012). QSEN competencies: A bridge to practice. *Nursing Made Incredibly Easy!, 10*(5), 1–3. https://doi.org/10.1097/01.NME.0000418040.92006.70

Jilka, S. R., Callahan, R., Sevdalis, N., Mayer, E. K., & Darzi, A. (2015). "Nothing about me without me": An interpretative review of patient accessible electronic health records. *Journal of Medical Internet Research, 17*(6), e161. https://doi.org/10.2196/jmir.4446

Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). Cyber threats to health information systems: A systematic review. *Technology and Health Care, 24*(1), 1–9. https://doi.org/10.3233/THC-151102

McCarthy, J. (2015, September 17). Healthcare leads all industries in data breaches. Retrieved from https://www.healthcareitnews.com/news/healthcare-leads-all-industries-data-breaches

McDermott, D. S., Kamerer, J. L., & Birk, A. T. (2019). Electronic health records: A literature review of cyber threats and security measures. *International Journal of Cyber Research and Education, 1*(2), 42-49.

Namoglu, N., & Ulgen, Y. (2013). Network security vulnerabilities and personal privacy issues in healthcare information systems: A case study in a private hospital in Turkey. *Informatics, Management, and Technology in Healthcare, 190,* 126–128.

National Council of State Boards of Nursing. (n.d.). Transition to practice course 5: Informatics v1.4. Retrieved from https://ncsbn-external.myabsorb.com/#/online-courses/ccc8b88b-99bf-40a6-b5a9-d866123b44e4

National Council of State Boards of Nursing. (2015). NCLEX-RN® detailed test plan: Item writer/item reviewer/nurse educator version. Chicago, IL: Author.

Parikh, C. (2018, February 1). Safeguarding electronic protected health information: A non- techie guide for healthcare leaders. *Healthcare Financial Management.* Retrieved from https://www.hfma.org/Content.aspx?id=59159

Seckman, C. (2018). Summer institute in nursing informatics 2018 balancing digital demands: Access, use security. *CIN: Computers, Informatics, Nursing, 36*(11), 521–524. https://doi.org/10.1097/CIN.0000000000000490

Spector, N., & Kappel, D. M. (2012). Guidelines for using electronic and social media: The regulatory perspective. *Online Journal of Issues in Nursing, 17*(3), 1.

U.S. Department of Health & Human Services (HHS). (2018). HHS cybersecurity program: Leadership for IT security & privacy across HHS. Retrieved from https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/information-security-privacy-program/index.html

U.S. Department of Health & Human Services (HHS). (2019). *Cybersecurity Awareness Training FY2019.* Retrieved from https://www.hhs.gov/sites/default/files/hhs-etc/security-awareness/index.html

Wanyonyi, E., Rodrigues, A., Abeka, S., & Ogara, S. (2017). Effectiveness of security controls on electronic health records. *International Journal of Scientific & Technology Research, 6*(12), 47–54.

Wilburn, A. (2018). Nursing informatics: Ethical considerations for adopting electronic records. *NASN School Nurse, 33*(3), 150–153. https://doi.org/10.1177/1942602X17712020

World Medical Association. (2016). WMA statement on cyber-attacks on health and other critical infrastructure. *World Medical Journal, 62*(4), 145–146.

Jessica L. Kamerer, EdD, MSN, RNC-NIC, is Associate Professor, Department Head of Nursing at Robert Morris University School of Nursing and Health Studies, Moon Township, Pennsylvania. **Donna McDermott, PhD, RN, CHSE,** is Associate Professor of Clinical, Assistant Dean, Simulation Programs at University of Miami School of Nursing and Health Studies, Miami Florida.