Open access publishing

COLUMBUS
PUBLISHERS PVT LTD

International Journal of Nursing and Health Care Science

Review Article

Aselton P, et al. J Int J Nurs & Healt Car Scie 04: 2024-299

Nurses Experience with Privacy of Electronic Health Record System

Pamela Aselton PhD, MPH, APRN[1#], Joohyn Chung PhD, MStat, RN[1], Amelia Bailey MPH[2]

[1#]Elaine Marieb College of Nursing, University of Massachusetts Amherst, Massachusetts, USA
[2]School of Public Health, Brown University, Rhode Island, USA

[#]**Corresponding author:** Pamela Aselton PhD, MPH, APRN, Clinical Associate Professor, Elaine Marieb College of Nursing, University of Massachusetts Amherst, Massachusetts, Amherst, Massachusetts 01003, USA

Submission Date: 07 January, 2024
Accepted Date: 22 January, 2024
Published Online: 25 January, 2024

How to cite this article: Aselton P, et al. (2024) Nurses Experience with Privacy of Electronic Health Record System. *Int J Nurs & Healt Car Scie* 04(01): 2024-299.

Abstract

Objectives: The purpose of this study was to explore nurses' experiences on privacy issues in the EHRs among faculty and nurses attending graduateprograms.
Methods: A mixed-method design was conducted using an online survey that combined qualitative and quantitative questionnaires. A convenience sample of 49 participants (34 nursing graduate students and 15 nursing faculty) responded. Quantitative data were descriptively analyzed, and qualitative data were disassembled and grouped according to meaning, reassembled, discussed, and interpreted by the first and second authors.
Results: one-fourth of nursing faculty (n=4, 27%) and one-fifth of nurses at graduate programs (n=6, 18%) reported a problem in protecting patients' personal information with more graduate nurses (67%) working in outpatient settings experiencing it than those in medical centers. From qualitative data, three themes emerged (1) mishandling access, (2) security and data breaches and (3) awareness of prevention measures for greater privacy.
Conclusions: Privacy protections for EHRs are not consistently implemented and data from smaller clinics may be more at risk than larger medical centers.

Background

Many healthcare providers and governments have been challenged to maintain patient data privacy in electronic health records systems (EHRs) and instituted security protocols to prevent them [1]. Privacy concerns include unauthorized persons receiving Personal Health Information (PHI) information that they are not given permission to view, and financial information being stolen or lost [2]. Personal Health Information includes names, addresses, Social Security numbers, financial accounts, biometric data, facial images, x-rays or diagnostic studies, and medical notes. Any unwarranted access to this data, as well as not following data handling procedures, put patients' information at risk.

Not following the security protocols at institutions may result in breaches of information, and healthcare team members need consistent and ongoing education in data security. Information in EHR systems is required to be stored securely, and only authorized users with a need to see medical information should be able to access it.

In an analysis of data breaches in healthcare from 2015 to 2017, internal staff (58%) were seen as the biggest threat, however more recent reviews have identified hacking or the installation of malware, more specifically ransomware, as the biggest threats followed by unauthorized internal disclosures [3].

These outside breaches are happening with increasing frequency as health data is seen as a valuable commodity. A 2021 data breach report performed by Verizon noted an increase in the hacking and malware type of attacks, but also expressed concern about the continued threat from those inside institutions either accessing PHI for illegal gain or due to curiosity or by having their credentials stolen from malware and used to access sensitive information.

Steps are being taken to prevent systemic attacks such as the Association of Information Systems initiated Bright ICT as a preventive security paradigm [4,5]. The initiative includes the development of relevant technology, public policies, social norms, international agreements, and measures through systematic research [6].

Purpose

The purpose of this study was to explore nurses' perceptions and experiences on privacy issues in the EHRs, by comparing nursing faculty and nurses attending graduate programs at a College of Nursing. Nurses and nursing faculty who use EHRs for work and may access their own patient portals are in a unique position to express views regarding privacy issues EHRs in patient care. Nursing faculty may work in health care systems clinically or supervise students that do and are familiar with both methods taken to ensure security and the actual day-to-day practice of maintaining security.

Methods

Research Design

A cross-sectional exploratory mixed-methods design using an online survey was used to explore nurses' views on privacy issues and protecting data in the EHR, as well as any experiences they might have had involving privacy breaches. After the approval of the University IRB, participants were invited via email using the college email listserv with a consent form and link to a Qualtrics survey. The survey consisted of Likert scale questions and several open-ended questions regarding participant experiences with protecting data in the EHR and any experiences they might have had involving data breaches.

Sample and settings

The target population included nurses enrolled in graduate programs and nursing faculty who often maintain clinical practice and supervise students at medical centers from one College of Nursing. The pool was about 250 individuals with 49 participants (34 nursing graduate students and 15 nursing faculty) responding.

Procedures

Upon the Institutional Review Board (IRB) approval from the University of the investigators, the study was performed virtually using the Qualtrics platform. The populations targeted received an email using the College of Nursing email listserv. The email contained a secure link to the Qualtrics platform. Consent was obtained through a cover letter which also included information about the survey.

Measures

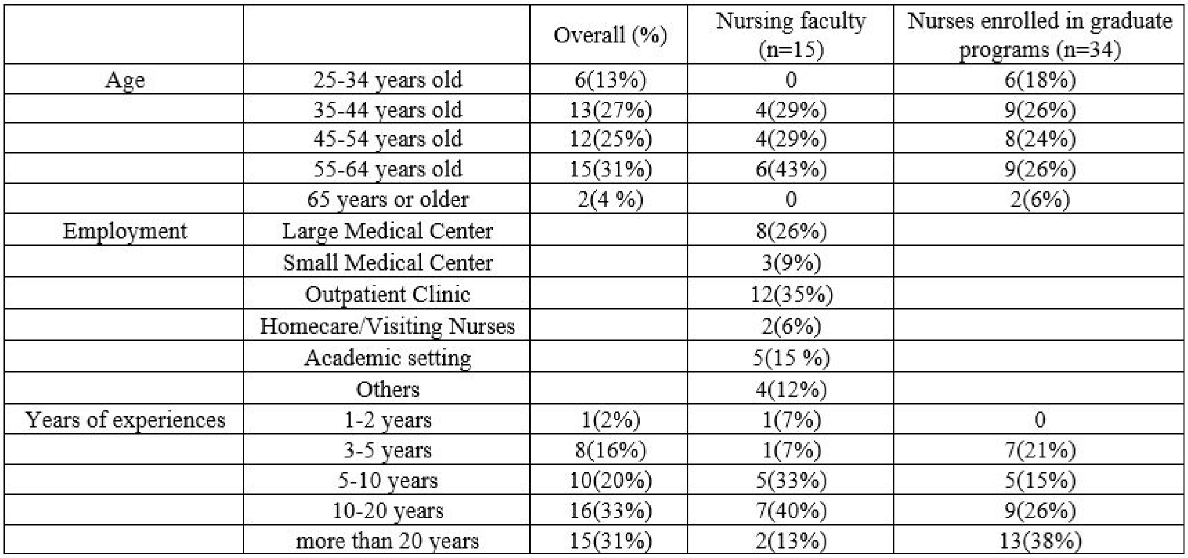
A survey developed by the research team was utilized. Six demographic questions (e.g., age, education, employment), eight open-ended questions, and two Likert scale questions were included to explore nurses' experience with protecting data in the EHR and any experiences they might have had involving data breaches.

Data Analysis

Analysis of the quantitative data was performed using SAS Version 9.4 (SAS Inc., Cary, NC). Quantitative data were descriptively analyzed and were presented using frequency (percentage) or mean (standard deviation, SD). Responses to open-ended questions were compiled for thematic analysis. After collecting statements, responses were disassembled and grouped according to meaning, reassembled, discussed, and interpreted by the first and second authors [7].

Results

Participants' Demographic Characteristics: Among the total of 49 participants, one-third of the participants were nursing faculty (n=15, 31%), and two-thirds of the participants were nursing graduate students (n=34, 69%, (Table 1)).



		Overall (%)	Nursing faculty (n=15)	Nurses enrolled in graduate programs (n=34)
Age	25-34 years old	6(13%)	0	6(18%)
	35-44 years old	13(27%)	4(29%)	9(26%)
	45-54 years old	12(25%)	4(29%)	8(24%)
	55-64 years old	15(31%)	6(43%)	9(26%)
	65 years or older	2(4 %)	0	2(6%)
Employment	Large Medical Center		8(26%)	
	Small Medical Center		3(9%)	
	Outpatient Clinic		12(35%)	
	Homecare/Visiting Nurses		2(6%)	
	Academic setting		5(15 %)	
	Others		4(12%)	
Years of experiences	1-2 years	1(2%)	1(7%)	0
	3-5 years	8(16%)	1(7%)	7(21%)
	5-10 years	10(20%)	5(33%)	5(15%)
	10-20 years	16(33%)	7(40%)	9(26%)
	more than 20 years	15(31%)	2(13%)	13(38%)

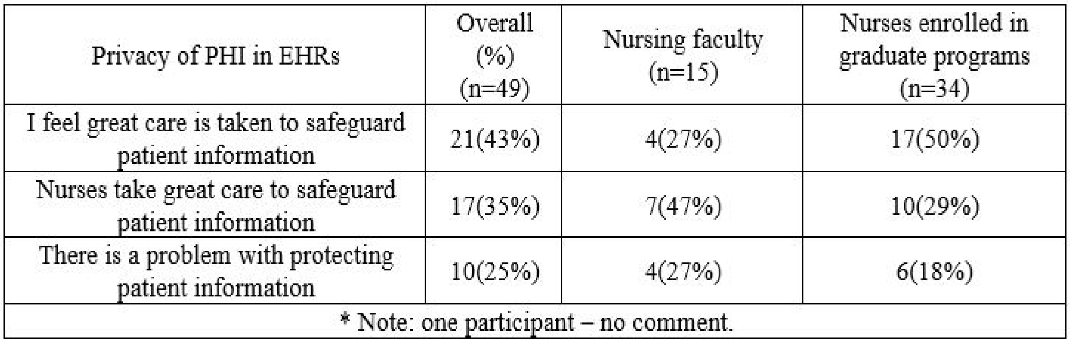
Table 1: Demographics of Participants.

The participants' ages ranged from 35 to 64 years old. Two-fifths of nursing faculty participants and one-third of nurses enrolled in graduate programs were older than 55 years and most (n=31, 64%) had more than 10 years of experience. Most of the graduate nursing students were employed at large medical centers (n=8, 26%) or at outpatient clinics (n=12, 35%, (Table 1)).

Quantitative Findings

Participants Views on Privacy

The following table presents the overall views on privacy by all participants, both nursing faculty and graduate nursing students. Approximately one-third of faculty (n=4, 27%) felt patient information was secure, and almost half of the nursing faculty (n=7, 47%) felt that nurses took great care in protecting patient information. However, four nursing faculty (27%) felt there was a problem in protecting patients' personal information. Although most graduate students (n=27, 79%) responded that patient information was safe and secure, one-fifth (n=6, 18%) expressed concern about protecting patient information (Table 2).

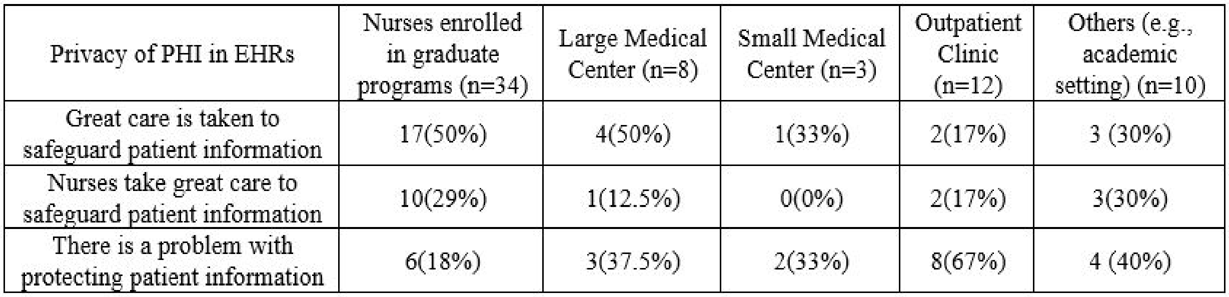


Privacy of PHI in EHRs	Overall (%) (n=49)	Nursing faculty (n=15)	Nurses enrolled in graduate programs (n=34)
I feel great care is taken to safeguard patient information	21(43%)	4(27%)	17(50%)
Nurses take great care to safeguard patient information	17(35%)	7(47%)	10(29%)
There is a problem with protecting patient information	10(25%)	4(27%)	6(18%)
* Note: one participant – no comment.			

Table 2: The Privacy of PHI in EHRs between Graduate Students and Faculty.

Graduate Nursing Students' perceptions of Privacy in the Workplace

The graduate nursing students who are mostly working full-time in a clinical setting were asked to identify their perceptions on privacy and to identify the setting they worked in presented in (Table 3) below.



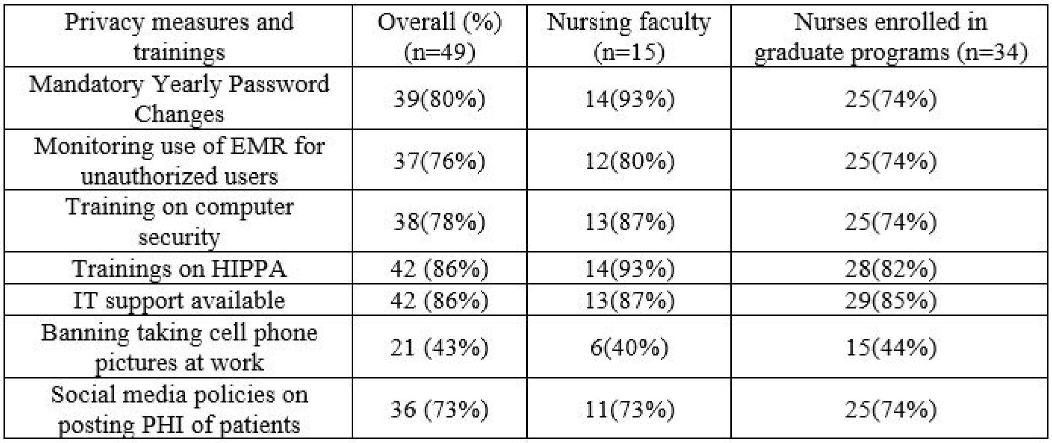
Privacy of PHI in EHRs	Nurses enrolled in graduate programs (n=34)	Large Medical Center (n=8)	Small Medical Center (n=3)	Outpatient Clinic (n=12)	Others (e.g., academic setting) (n=10)
Great care is taken to safeguard patient information	17(50%)	4(50%)	1(33%)	2(17%)	3 (30%)
Nurses take great care to safeguard patient information	10(29%)	1(12.5%)	0(0%)	2(17%)	3(30%)
There is a problem with protecting patient information	6(18%)	3(37.5%)	2(33%)	8(67%)	4 (40%)

Table 3: Perceptions of Privacy by Setting of Graduate Nursing Students.

Based on 34 Nursing Graduate Students

While half of the graduate nursing students surveyed (n=17, 50%) felt that patient information was safe and secure, one-fifth of nurses at graduate programs (n=6, 18%) indicated there was a problem with protecting patients' personal health information. One-third (n=10, 29%) responded that nurses protected PHI from third parties without their consent. Among those who worked at the large medical centers, three nurses (37.5%) responded that there was a problem with protecting patient information. However, among those who worked at the outpatient clinics, more than half of the nurses (n=8, 67%) working in outpatient settings felt there was a problem patients' PHI in their setting.

In terms of privacy measures taken at work, most participants changed passwords yearly (80%), had EMRs monitored for unauthorized users (76%), had training on HIPAA (86%) and IT support (86%). Most worksites had social media policies (73%) and picture bans (43%) as demonstrated in (Table 4).



Privacy measures and trainings	Overall (%) (n=49)	Nursing faculty (n=15)	Nurses enrolled in graduate programs (n=34)
Mandatory Yearly Password Changes	39(80%)	14(93%)	25(74%)
Monitoring use of EMR for unauthorized users	37(76%)	12(80%)	25(74%)
Training on computer security	38(78%)	13(87%)	25(74%)
Trainings on HIPPA	42 (86%)	14(93%)	28(82%)
IT support available	42 (86%)	13(87%)	29(85%)
Banning taking cell phone pictures at work	21 (43%)	6(40%)	15(44%)
Social media policies on posting PHI of patients	36 (73%)	11(73%)	25(74%)

Table 4: Privacy measures at workplaces.

Qualitative Findings

The following three themes were identified with examples of statements below: mishandling of records both in terms of access and legal issues,' data breaches and how institutions handle them as well as patient privacy concerns, and finally prevention measures for greater privacy.

1. a. The first theme of 'Mishandling Access' was defined as access without the necessary care, including workers accessing records they should not look at.

Many participants shared experiences of mishandling related to accessing patient information.

"My director looked at my healthcare record to see when I would return to work."

"Family member denied a job when hiring supervisor accessed medical record."

" You hear about people who have tried to get into relatives' or friends' records.

"Yes, medical information is discussed in the medical department when unauthorized medical personnel are present.

"Yes, nurse looking up information on a colleague."

"Yes, other staff accessing PHI of friends and family members without consent."
"Yes- a nurse that I used to work with accessed the EHR of another employee while she was an active patient in the ED. This chart was audited, the nurse was called in for a compliance meeting, and she was offered to resign or otherwise would have been terminated. She chose to resign on her own."

"A famous kidnapping victim had over 100 unauthorized view of hospital record".

"Yes, I work at an organization that often cares for well-known personalities and I have seen staff violate their privacy, but I have also seen them fired for doing so!"
"Yes, there was a time when one of our MDs was sick and a bunch of employees went in the medical record. They were fired if there was no reason to be in there."

b. The theme 'Security and Data Breaches' was identified as a wide array of the process of protecting data from unauthorized access and data breaches. *Participant responses illustrated how institutions' management of intrusion varies.*

"Yes, I have received letters that my PHI had been jeopardized with no repercussions that I am aware of. I know that staff have been fired when it was reported that they were looking at records inappropriately. The safety officer or that department will first run a report on an individual's access and if the access was appropriate. Then if the complaint is valid it is dealt with, often the result is termination."

"Yes, once I was a patient at the facility where I was working, and my director looked at my healthcare record to estimate when I would return to work. I know that this occurred because she repeated things that I had only mentioned to my healthcare provider and had not shared with anyone. There were not any repercussions, but I never trusted her again."

"Yes. The health care facility said, "some records were accessed". No repercussions thus far."

2. Patient Privacy Concerns were defined as improper maintenance that might be caused by a failure to follow the established protocols or practice manuals Participants shared confidentiality concerns on units and at home.

"Yes. I have seen medical records of other patients left in plain sight both when as a patient and working as a nurse."

"I have experienced other providers not maintaining confidentiality within the office due to being over comfortable within the setting and using patients' names and chief complaints in the hall in front of other staff and other patients/families."

"I think that it is common for clinicians to view a medical record that is not technically necessary in order to treat...but very rarely is it done for someone completely out of their unit/department, etc."

"In the NICU, rounds are performed by other infant bedspaces, where families sit. Parents of other children have asked me questions about patients because of overhearing what was discussed during rounds."

"During COVID 19 it is more important than ever to protect PHI. At present, I am back in the office so this is not an issue. But during the COVID lock down, I did have to restrict my partner from my home study, which was a challenge, he sees this space as his house. He complied. For this reason, I prefer to work at work!"

Awareness of Prevention Measures for Greater Privacy -
Participants had opinions on what more needed to be done and were aware of several measures to ensure PHI privacy. Although these are legally required, not all may not be implemented consistently in workplaces.

Patient's records should not be routinely accessed from providers' homes or personal devices."

"Prevention methods-active monitoring and limited access with break the glass type access points. At home do not store passwords and use different passwords for different sites."

"I think the main things are making the firewalls as strong as possible and really impressing upon employees that if they ever print anything with PHI it MUST be kept in a folder with their name and phone number on it (e.g. "CONFIDENTIAL: if found, please return to -------- at 555-5555), should NEVER be left on public desk or workspace, and must be reported missing immediately if they lose it "

"Limit the information that can be easily printed. Enlarge the screens on handheld devices so that it is easier to read the information. I try to protect my information at home by using a shredder, using unique passwords, and working from my laptop at home rather than my phone."

"Remind staff not to leave their access available on the portable computers in the hallways. Secure passwords and pay for added protection.

Many of the participants mentioned steps they take at home to protect their own information, such as shredding paper documents with PHI and financial information, avoiding certain websites and insecure browsers, and trying to have a secure password for their accounts. Some even expressed concern about working with EHRs at home and wanted to make sure they were encrypted and made efforts to keep family members away from the computer.

Discussion

This study explored nurses' experiences with privacy issues in the EHRs among faculty and nurses attending graduate programs. Among a total of 49 participants (15 nursing faculty and 35 nurses at graduate programs), the majority of them were older than 55 years (two-thirds of nursing faculty and one-third of nurses at graduate programs), and had more than 10 years of experience (a half of nursing faculty, and two-third of nurses at graduate programs). From quantitative findings, the majority of both nursing faculty and nurses at graduate programs reported that patient information was safe and secure. However, about 25%-30% of both nursing faculty and nurses in graduate programs reported there was a problem with protecting patient information. Specifically a variety of instances where security protocols were not consistently used.

Similarly, qualitative findings support that several concerns were expressed, although most of the graduate student nurses agreed that their worksites were secure and nurses protected patient data. Incidents of unauthorized access did not always result in repercussions or the ability of supervisors to look at their medical records. No one reported an incidence of ransomware at their site, and no one was aware of malware picking up their sign in information.

Concerns about non-medical personnel accessing medical records they were required to submit was a particular concern of nursing faculty. This access could have to do with nursing faculty having to submit clinical reports of physicals and immunizations to get cleared for clinical sites and feeling uncomfortable with those personal documents being within the possession of human resources or on a secure online commercial database. Faculty also reported incidents of unauthorized access to patient information at clinical facilities they were familiar with.

Current literature has been addressed improper EHRs (Electronic Health Records System) resources sharing, when Personally Identifiable Information (PII) or Protected Health Information (PHI) is shared without patient approval, as the form of a data breach [8,9]. Many organizations have been made to protect against unauthorized access to PHI [10,11]. The U.S. Department of Health and Human Services (HHS) has strengthened its oversight of privacy and security to healthcare facilities, due to the increased use of electronic health records systems, cloud computing systems, and the Internet of things (IoT). Yet, data breaches still impacted many individuals. Most of data breaches originated at third-party vendors with to PHI [1,8,11-14]. Access by family members and roommates has not been emphasized for privacy training as much as it should be.

There is a critical need for implement strong strategies to manage third-party risks for data breaches. In addition, meaningful prevention measure and security protocols for greater privacy are emphasized such as systematic monitoring and auditing protocol adherenece and the use of specific prevention measures [12,15,16]. It is important for all members of the healthcare team to be vigilant regarding patient privacy in the EHR, regardless of settings and size of facilities.

Workplace safeguards for the privacy of EHRs' PHI were reported by the participants as generally good, for example, most completed yearly password changes, HIPAA trainings, and have adequate IT (Information Technology) support. Many clinical sites ban photos and have social media policies against posting patient information online. In this study, nurses working in outpatient clinics reported more concerns about patient privacy, compared with others working in large/small medical centers. Previous studies also supported that outpatient clinics may have more of a data breach problem than large medical centers, which may have more resources in terms of IT and security [17]. In this small set of data this did appear to be the case. A greater percentage of nurses working in outpatient clinics (67%) reporting a problem with how private PHI was than in large medical centers (37%) or small medical centers (33%). It could be that smaller clinics do not have adequate information technology specialists to monitor access to PHI, or a lack of training for staff. For smaller providers and clinics, it is critical to provide regular training to providers and staff, and to provide adequate IT supports to ensure patient privacy, rather than only to regulate for violations.

Healthcare professionals need to be mindful of sharing personal information online which may lead to the stealing of professional identities and keep up to date with security updates to protect PHI and their identities online. The literature indicates a problem with criminal groups stealing professional identities to enter secure EHR systems, and this must be avoided at all costs [3].

Many organizational efforts have been made to protect PHI privacy through public awareness campaigns, clinicians and staff training, work process redesign, and increased IT support [18-21]. A recent effort was utilizing algorithms to operate without the need to share original data across sites, such as logistic regression, Cox regression, and principal component analysis [20-24]. As earlier mentioned, the Bright Information and Communication Technology (ICT) platforms have emerged for the future foundation across borders since 2014. The initiative continues to create many research opportunities to make efficient and effective infrastructures and communication platforms. The privacy protections in EHRs need to be congruent with the Bright ICT platforms, based on understanding patients' health information rights.

One of the study's strengths was the experienced group of nurses from around the country sharing their thoughts on the privacy of personal health information in EHRs as both a patient and clinician. Limitations included the nature of descriptive data collection, which is not an accurate measurement tool of a large population of nurses and the small sample size which might make it difficult to justify the results. Also, some of the comments on privacy were based on hearing of incidents that happened to other people and not experienced directly by the nurses. For future studies, it would be recommended to have a large sample with different settings and other healthcare professionals included.

Conclusions

The advent of the widespread use of EHRs has had enormous benefits for many aspects of healthcare: including clinical decision-making, research, billing, and pharmacy, however there is still a threat to privacy unless safeguards are consistently followed and updated. The nurses surveyed for this study all had training in protecting that security, but it did not appear to be consistently followed in terms of monitoring unauthorized access or limiting access to supervisors of employees' medical records. That may have negative consequences for those seeking employment or those already employed at an institution. The problem of looking at medical records while working at home may become more of an issue with more telehealth and work-from-home positions. Access by family members and roommates has not been emphasized for privacy training as much as it should be. It is important for all members of the healthcare team to be vigilant regarding patient privacy in the EHR in whatever setting they are working in.

References

1. Hathaliya JJ, Tanwar S. (2020) An exhaustive survey on security and privacy issues in Healthcare 4.0. Computer Communications 153: 311-335.
2. Vinaykumar SZ, Chi; Shahriar Hossain (2019) Security and Privacy of Electronic Medical Records. presented at: SAIS 2019 Proceedings.
3. Seh AH, Zarour M, Alenezi M, et al. (2020) Healthcare Data Breaches: Insights and Implications. Healthcare (Basel) 8.
4. Lawrence VB, Ayaburi EW, Andoh-Baidoo FK, et al. (2022) Editorial: Special Issue on "Bright ICT: Security, Privacy and Risk Issues". Inf Syst Front 1-4.
5. Lee J, Cho D, Lim G. (2018) Design and Validation of the Bright Internet. Journal of the Association for Information Systems 19: 63-85.
6. Association for Information System. (2022) Bright ICT Initiative. Association for Information System.
7. Castleberry A, Nolen A (2018) Thematic analysis of qualitative research data: Is it as easy as it sounds? Curr Pharm Teach Learn 10: 807-815.
8. Choi SJ, Johnson ME, Lehmann CU (2019) Data breach remediation efforts and their implications for hospital quality. Health Serv Res 54: 971-980.
9. Shi J, Wang D, Tesei G, et al. (2022) Generating high-fidelity privacy-conscious synthetic patient data for causal effect estimation with multiple treatments. Front Artif Intell 5: 918813.
10. Walden A, Cortelyou-Ward K, Noblin A (2021) Privacy Officers: Who They are and Where They Work. Perspect Health Inf Manag. Spring 18:1.
11. Services USDoHH (2022) Health Information Privacy: Breach Notification Rule.
12. Bechade C, Lanot A, Guillouet S, et al. (2022) Impact of assistance on peritonitis due to breach in aseptic procedure in diabetic patients: A cohort study with the RDPLF data. Perit Dial Int 42: 185-193.
13. Edemekong PF, Annamaraju P, Haydel MJ (2022) Health Insurance Portability and Accountability Act. StatPearls.
14. Hekel R, Budis J, Kucharik M, et al. (2021) Privacy-preserving storage of sequenced genomic data. BMC Genomics 22: 712.
15. Bani Issa W, Al Akour I, Ibrahim A, et al. (2020) Privacy, confidentiality, security and patient safety concerns about electronic health records. Int Nurs Rev 67: 218-230.
16. Hasan MZ, Mahdi MSR, Sadat MN, et al. (2018) Secure count query on encrypted genomic data. J Biomed Inform. May 81: 41-52.
17. Aselton PJ AS (2014) Privacy Issues with the Electronic Medical Record. Annals of Nursing and Practice 1: 1009.
18. Arvisais-Anhalt S, Lau M, Lehmann CU, et al. (2022) The 21st Century Cures Act and Multiuser Electronic Health Record Access: Potential Pitfalls of Information Release. J Med Internet Res. Feb 17: e34085.
19. Basil NN, Ambe S, Ekhator C, et al. (2022) Health Records Database and Inherent Security Concerns: A Review of the Literature Cureus 14: e30168.
20. Hall JN, Ackery AD, Dainty KN, et al. (2022) Designs, facilitators, barriers, and lessons learned during the implementation of emergency department led virtual urgent care programs in Ontario, Canada. Front Digit Health 4: 946734.
21. Yang M, Zhang C, Wang X, et al. (2022) TrustGWAS: A full-process workflow for encrypted GWAS using multi-key homomorphic encryption and pseudorandom number perturbation. Cell Syst. 13: 752-767 e6.
22. Chen AA, Luo C, Chen Y, et al. (2022) Alzheimer's Disease Neuroimaging I. Privacy-preserving harmonization via distributed ComBat. Neuroimage 248: 118822.
23. Duan R, Boland MR, Liu Z, et al. (2020) Learning from electronic health records across multiple sites: A communication-efficient and privacy-preserving distributed algorithm. J Am Med Inform Assoc 27: 376-385.
24. Duan R, Luo C, Schuemie MJ, et al. (2020) Learning from local to global: An efficient distributed algorithm for modeling time-to-event data. J Am Med Inform Assoc 27: 1028-1036.