CIN: Computers, Informatics, Nursing • Vol. 33, No. 2, 58–62 • Copyright © 2015 Wolters Kluwer Health, Inc. All rights reserved.

CONTINUING EDUCATION

CE 2.0 ANCC Contact Hours

Is Patient Confidentiality Compromised With the Electronic Health Record?

A Position Paper

ILSE M. WALLACE, MS, RNC

In order for electronic health records to fulfill their expected benefits, protection of privacy of patient information is key. Lack of trust in confidentiality can lead to reluctance in disclosing all relevant information, which could have grave consequences. This position paper contemplates whether patient confidentiality is compromised by electronic health records. The position that confidentiality is compromised was supported by the four bioethical principles and argued that despite laws and various safeguards to protect patients' confidentiality, numerous data breaches have occurred. The position that confidentiality is not compromised was supported by virtue ethics and a utilitarian viewpoint and argued that safeguards keep information confidential and the public feels relatively safe with the electronic health record. The article concludes with an ethically superior position that confidentiality is compromised with the electronic health record. Although organizational and governmental ways of enhancing the confidentiality of patient information within the electronic health record facilitate confidentiality, the ultimate responsibility of maintaining confidentiality rests with the individual end-users and their ethical code of conduct. The American Nurses Association Code of Ethics for nurses calls for nurses to be watchful with data security in electronic communications.

KEYWORDS

Code of Ethics • Confidentiality • Electronic health record • Nurse • Privacy

Nurses have the ethical obligation to protect their patients' private health information. Are electronic health records (EHRs) compromising patient confidentiality despite laws and professional codes of conducts that protect patients' privacy and confidentiality? Are EHRs making patient information too accessible, or are they just as safe or even safer than traditional paper records? This article investigates the ethical issue of patient confidentiality as it relates to the EHR. An analysis of the ethical issue is first presented; then, two opposing positions are described and supported; and finally, one position is suggested as the superior ethical position from the standpoint of the nursing profession.

CONFIDENTIALITY AND THE ELECTRONIC HEALTH RECORD

The EHR presents many benefits. At its full capacity, it is intended to improve patient-centered care and coordination of care through enhanced access to patients' health information by all members of the healthcare team.[1] Furthermore, deidentified information can be used to benefit public health and to conduct research.[2] However, in order for the EHR to fulfill its expected benefits, protection of privacy and safety of patient health information is key. If patients do not trust that their health information is kept confidential, they may be reluctant to be honest or fully disclose all relevant information, which could have potentially grave consequences in their care.[3] As frontline users of the EHRs, nurses are both ethically obligated and in a key position to protect patient confidentiality.

The key issue that has the potential to compromise patients' privacy in EHRs is that all information that has been once entered will be stored in longitudinal records forever, even though it may never again be relevant in caring

Author Affiliation: Nursing, Palm Beach State College, Lake Worth; and College of Nursing and Health Sciences, Barry University, Miami Shores, FL.

This article is an original contribution not published or in consideration for publication elsewhere in this or similar form or in any other language.

The author has disclosed that she has no significant relationships with, or financial interest in, any commercial companies pertaining to this article.

Corresponding author: Ilse M. Wallace, MS, RNC, Nursing, Palm Beach State College, 4200 Congress Avenue, Lake Worth, FL 33461 (wallacei@palmbeachstate.edu).

DOI: 10.1097/CIN.0000000000000126

for the patient.[4] Although patients' confidentiality may be compromised because of computer issues, such as inadequate protection or lack of encryption of the data, most breaches have occurred because healthcare professionals have unwittingly accessed or shared patient information.[5] Laws such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) protect patients' privacy and confidentiality through compliance and breach notification requirements for healthcare organizations and healthcare practitioners.[6] The US Department of Health and Human Services recently released a new rule to enhance the HIPAA of 1996.[7] The new ruling will help protect patient privacy with added enforcement of the HIPAA compliance especially as it relates to the HITECH Act and the EHR.[7]

In addition, healthcare professionals' codes of conduct outline the duties of individual practitioners in protecting patients' privacy and confidentiality. The Code of Ethics for nurses by the American Nurses Association (ANA) was provisionally adopted in 1926 and fully adopted in 1950; however, the 1893 "Nightingale Pledge… is understood as the first nursing code of ethics."[8(p27)] The Code of Ethics provides a framework for nurses in making decisions that are ethical and in line with the professional duties expected of a nurse.[8] In the ANA Code of Ethics for nurses, privacy is a patient right, while confidentiality refers to the duty of a nurse. In its interpretive statements, provision 3 in the ANA Code of Ethics discusses the privacy and confidentiality of patient information: "The nurse safeguards the patient's right to privacy… and the nurse has a duty to maintain confidentiality of all patient information."[8(p12)] The International Council of Nurses also has a code of ethics for nurses, which outlines the ethical conduct of confidentiality by stating, "The nurse holds in confidence personal information and uses judgment in sharing this information."[9(p2)]

In order to illuminate the ethical issues with patient confidentiality and the EHR, the following fictitious situation that nurses may witness or participate in is presented. In the situation, a nurse is in the middle of administering medications to his patient in a room full of visitors. He has logged into the computer and begins to scan the medications when he realizes that he forgot to retrieve one medication from the medication dispenser located in the medication room. Because it will only take him a minute to get the medication and the computers take longer with the re-login process, he decides to just turn the monitor screen off, which is what pretty much everyone does on the unit when they have to leave their computer station just for a minute.

POSITION IN FAVOR

The position in favor asserts that EHRs do compromise the confidentiality of patients' health information. There is always a possibility for patient confidentiality to be compromised with EHRs. During the paper age, mere physical security, such as locked rooms, to protect medical records was typically sufficient; however, the digital age has significantly increased potential unauthorized access to patient information. While breaches in confidentiality certainly occurred in the paper era, those exchanges would have been limited. The fact that paper records are physically relatively difficult to access, especially beyond a few records, protects the patient information within them.[10] Electronic health records are a new threat to the protection of patients' privacy. Technological advancements, such as computerized health records, have "opened the door to potential, unintentional breaches of private/confidential health information."[11(p1)] Protecting patients' private health information is extraordinarily difficult within an EHR, which holds complete and integrated information in a longitudinal fashion.[12] The Inspector General report concluded that EHRs lack safeguards.[13] There are increasing reports of instances where confidentiality of patient information has been compromised, some of which have been high-profile cases displayed in the media.[14] Since 2012, there has been a 138% increase in HIPAA data breaches, and the total number of health records that have been compromised since 2009 is 29.3 million.[15] According to the Ponemon Institute's (2014) benchmark study of 91 hospitals' privacy and security of data, 75% of hospitals reported that data breaches occurred because of "employee negligence."[16(p12)]

A search of relevant literature across disciplines was conducted to explore the phenomenon of EHRs and patient confidentiality. Four research studies were reviewed in which the experience of EHRs and confidentiality was investigated. Strauss[17] conducted a qualitative phenomenological study exploring patients' experience of "the nurse-patient relationship when nurses utilize an EHR."[17(p596)] One of the themes that emerged was safety and trust. The patients were concerned about the easy access to their information and that others might use it incorrectly. They were also concerned that information about their drug addiction or mental illness could affect how their providers treat them. Lastly, they explained that there was a lack of consistency on the part of the nurses in describing how patient information was kept private within the EHR.[17] A qualitative study of 34 emergency department staff members, including doctors and nurses, investigated participant perceptions of accessibility and confidentiality of information within the EHR.[18] The participants felt that having access to patients' medical, occupational, and social information was important but expressed concerns about the confidentiality of patient information. One participant had witnessed staff members sharing user names and passwords, and another participant was worried about misuse by authorized staff members.[18] In a qualitative study of psychologists (N = 28) and the critical incidents relating to using technologies, such as EHRs, in mental health practice, the researchers found that among

the emerged themes were "unauthorized access to patient information… and inappropriate dissemination of client information via technology."[19(p433)] In a cross-sectional study of public (N = 1847) attitudes related to electronic health information exchange (HIE), the results indicated that a majority of participants were concerned about the privacy of HIE and the security of EHRs.[20] A large majority also agreed that the benefits outweigh the privacy risks and would allow the HIE in provider treatment even if their privacy were compromised. In addition, little over half of the participants wanted to be able to have a say on who would have access and be able to share their information.[20]

In analyzing the ethical issue of confidentiality and EHR, the four bioethical principles of autonomy, beneficence, nonmalfeasance, and justice may bring support for the position that EHRs do compromise patient confidentiality. The bioethical principles guide healthcare professionals in ethical decision making.[21] In the era of paper records, patients were able to control which health professionals had access to their information.[2] Now, depending on the design of the EHR, patients' control over access to their private information can be compromised,[2] and they are likely not even aware of who has viewed their information, for example, during a hospital stay. The ethical principle of autonomy is hence affected. Furthermore, there is particularly sensitive information that patients may not want shared among various healthcare professionals, such as mental health issues or imprisonment.[22,23]

Beneficence is the duty to do good, and nonmaleficence refers to the duty to do no harm.[21] The intention of the EHR is that of beneficence, or doing good to patients through better collaboration and exchange of information among healthcare professionals. However, if patients avoid care or are not honest in the disclosure of information because of fear of possible breach in confidentiality, the potential for nonmaleficence is present. "Doctors may unwittingly base diagnoses on false or misleading information, leading to treatment decisions that are not in the patient's best interest or that cause actual harm."[2(p9)] The principle of justice refers to all patients being treated equally.[21] The lack of trust in the confidentiality of health information has the potential to affect people disproportionately. For example, individuals who have been victims of sexual assault or domestic abuse or whose conditions are stigmatized by society, such as is the case with AIDS and mental illness, may be especially reluctant to seek care if they feel that confidentiality could be breached.[2] In the fictitious situation presented earlier, the potential was present, because the nurse left the EHR unattended, that a visitor could have accessed sensitive information that the patient would not have consented to, leading to patient harm. Hence, the nurse's action violated the ethical principles discussed, and patient confidentiality was compromised with the EHR.

POSITION AGAINST

The position against asserts that EHRs do not compromise the confidentiality of patient health information. When safeguards are present, such as encryption of the data, patient health information will be protected, even in case of theft or loss of a computer holding patient health records.[24] Other safeguards exist as well, such as audit trails, role-based access, compliance enforcement, and breach reporting.[25] While EHRs are not 100% safe, neither are paper records; in addition, the benefits of EHRs outweigh the risks.[26] Furthermore, breaches of confidentiality, such as unauthorized end-user disclosures, also occurred during the paper era, and although they may have been more difficult or limited because paper charts were relatively difficult to access, the fundamental nature of the breach is no different. Electronic health records in themselves do not compromise patient confidentiality. The issue seems to be more about a trusting relationship between healthcare providers and patients than about the EHR compromising patient confidentiality. Americans have ranked nurses as the most trusted profession since 2005, rating their honesty and ethical standards as high or very high.[27]

A search of relevant literature across disciplines was conducted to explore the phenomenon of EHRs and patient confidentiality. Three research studies were reviewed in which the experience of EHRs and confidentiality was explored. A recent telephone survey of 1015 participants within the United States revealed that the public is surprisingly trusting of confidentiality as it relates to the EHR.[28] The results revealed that whereas 40% of the participants were very concerned about privacy of their EHR, 22% were not concerned about privacy, 68% thought EHRs were secure, and 64% agreed that their benefits outweigh the risks.[28] In another study, only 4% of the 138 participants believed that EHRs led to the possibility of healthcare providers learning information about them that was not necessary for the provider to know.[28] These participants were most concerned about the possibility of hackers getting to their information.[29] Larsen[30] conducted a qualitative study of palliative care nurses' (N = 20) perceptions of using PDAs and computer-mediated communication in the daily care of their patients. The research centered on privacy and confidentiality issues. All of the nurses in the study "were concerned about safeguarding client information against unauthorized use"[30(p337)] but felt that superior security existed with computer-mediated communication when compared with information written in a paper form.

An individual who believes that EHRs do not compromise patients' confidentiality may be approaching his/her stance from a virtue ethics standpoint. In virtue ethics, what matters are the motives or intentions of the ethical agent: "The fundamental assumption underpinning practical applications of virtue ethics is that morally upstanding individuals

will, as a matter of course, act appropriately and in accordance with established rules and standards."[31(p17)] Virtuous healthcare professionals, from the virtue ethics viewpoint, would then be expected to act in confidentiality of patient information regardless of whether it is in an electronic or paper format. However, because not all individuals who have access to EHRs are virtuous, perhaps another ethical theory is needed to support the against position. One could also look at the ethical issue of confidentiality and EHR from a utilitarian ethical theory perspective. In utilitarianism, what matters most is "the greatest good for the greatest number of people."[21(p10)] A utilitarian perspective then would determine that if few individuals' EHRs were compromised, as long as the communities at large reaped benefits in areas such as public health and research, then the benefits of EHRs would outweigh the risks in regards to compromised confidentiality.

CONCLUSION

Confidentiality refers to the duty of individuals to protect the information that has been provided to them.[7] The ANA Code of Ethics draws specific attention to confidentiality with electronic communication by stating "when using electronic communications, special effort should be made to maintain data security."[7(p12)] Nurses would be unwise to preserve a specious sense of security regarding the EHR. Although EHRs in themselves may not compromise patient confidentiality, people do. An established fact is that breaches of confidentiality with the EHR are commonly end-user driven. The better ethical position for nurses, then, is to not solely trust that patient information is protected within the EHR because of organizational or governmental safeguards. While the organizational and governmental ways of enhancing the confidentiality of patient information within the EHR, such as audit trails, role-based access, encryption of data, antivirus software, compliance enforcement, and breach notification, facilitate confidentiality,[25] the ultimate responsibility lies with the individual end-users and their ethical code of conduct. Although hackers and criminals may be at the center of news stories, "well-meaning computer users can be their own worst enemies"[25(p13)] for various reasons, such as users being pressed for time or inadequate education. In the previously illustrated fictitious situation, the nurse's ethical code of conduct is at the center of making an ethically sound decision. Pressed for time, the nurse left the patient's EHR accessible to visitors. In order to preserve professional integrity and patient confidentiality, nurses should consistently log out of their workstations when not documenting, and they should never share their passwords with anyone.[5] "Nurses and other health professionals need to use their professional and employer codes of conduct to recognize when accessing a patient's information may be breaching patient privacy."[5(p32)]

Seemingly, the underlying issue for nurses to recognize is successfully translating governing regulations and professional ethical principles into practice. Therefore, as nurses, we cannot afford to assert that EHRs do not compromise patient confidentiality, simply based on virtue and utilitarian ethical perspectives or the regulations that have long been in place. Instead, we must refocus our efforts in safeguarding patient confidentiality to include the education, compliance, and monitoring of the end-users. As the frontline users of EHRs, nurses have the duty to not only individually protect patient confidentiality but also to be collectively involved in policies and practices to create an environment that is conducive to protecting patient privacy. "Nurses may need to leave organizations that refuse to support patient rights or put nurses in a position that consistently demands violation of the professional standards of practice."[32(p192)] The integrity of the nursing profession is upheld through the guidance of the ANA's Code of Ethics for nurses, maintaining high standards in nursing education to include students' value development and constant appraisal of nursing actions.[32]

REFERENCES

1. Garett P, Seidman J. EMR vs. EHR—what is the difference? 2011. http://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/emr-vs-ehr-difference/. Accessed May 8, 2014.
2. Carey CA, Stern G. Protecting patient privacy: strategies for regulating electronic health records exchange. 2012. http://www.nyclu.org/files/publications/nyclu_PatientPrivacy.pdf. Accessed May 8, 2014.
3. US Department of Health and Human Services. Nationwide privacy and security framework for electronic exchange of individually identifiable health information. 2008. http://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf. Accessed May 18, 2014.
4. Rothstein MA. Currents in contemporary bioethics. Access to sensitive information in segmented electronic health record. *J Law Med Ethics*. 2012;40(2):394–400.
5. Rolls S. Who needs to know? Think about the patient's privacy before you search and share. *Kai Tiaki Nurs N Z*. 2013;19(5):32.
6. American College of Healthcare Executives. Health information confidentiality. 2012. http://www.ache.org/policy/hiconf.cfm. Accessed September 7, 2014.
7. US Department of Health and Human Services. New rule protects patient privacy, secures health information. 2013. http://www.hhs.gov/news/press/2013pres/01/20130117b.html. Accessed May 17, 2014.
8. American Nurses Association. *Code of Ethics for Nurses With Interpretive Statements*. Silver Springs, MD: American Nurses Association; 2001.
9. The International Council of Nurses. The ICN Code of Ethics for Nurses. 2012. http://www.icn.ch/images/stories/documents/about/icncode_english.pdf. Accessed April 24, 2014.
10. Graves S. Confidentiality, electronic health records, and the clinician. *Perspect Biol Med*. 2013;56(1):105–125.
11. American Nurses Association. ANA position statements on ethics and human rights. Privacy and confidentiality. 2006. http://www.nursingworld.org/MainMenuCategories/EthicsStandards/Ethics-Position-Statements/PrivacyandConfidentiality.html. Accessed September 7, 2014.
12. Rothstein MA. The Hippocratic bargain and health information technology. *J Law Med Ethics*. 2010;38(1):7–13.
13. US Department of Health and Human Services. Not all recommended fraud safeguards have been implemented in hospital EHR technology. 2013. http://oig.hhs.gov/oei/reports/oei-01-11-00570.pdf. Accessed May 18, 2014.

14. Schultz D. As patients' records go digital, theft and hacking problems grow. 2012. http://www.kaiserhealthnews.org/Stories/2012/June/04/electronic-health-records-theft-hacking.aspx. Accessed May 8, 2014.
15. Redspin. Breach report 2013: Protected Health Information (PHI). 2014. http://www.redspin.com/docs/Redspin-2013-Breach-Report-Protected-Health-Information-PHI.pdf. Accessed May 18, 2014.
16. Ponemon Institute. Fourth annual benchmark study on patient privacy & data security. 2014. http://www.ponemon.org/blog/fourth-annual-benchmark-study-on-patient-privacy-and-data-security. Accessed May 17, 2014.
17. Strauss B. The patient perception of the nurse-patient relationship when nurses utilize an electronic health record within a hospital setting. *Comput Inform Nurs*. 2013;13(12):596–604.
18. Ayatollahi H, Bath PA, Goodacre S. Accessibility versus confidentiality of information in emergency department. *Emerg Med J*. 2009; 26:857–860.
19. Allen JV, Roberts MC. Critical incidents in the marriage of psychology and technology: a discussion of potential ethical issues in practice, education, and policy. *Prof Psychol Res Pract*. 2001;42(6):433–439.
20. Dimitropoulos L, Patel V, Scheffler SA, Posnack S. Attitudes toward health information exchange: perceived benefits and concerns. *Am J Manag Care*. 2011;17(12):111–116.
21. Fremgen BF. *Med Law Ethics*. Boston, MA: Pearson Prentice Hall; 2010.
22. Dunne JE, Sarvet B, Lambert K, Wertheimer M. New risks to confidentiality in the modern era. *Psychiatr Times*. 2012;29(12):32–34.
23. Goldstein MM. Health information privacy and health information technology in the US correctional setting. *Am J Public Health*. 2012; 104(5):803–809.
24. Kirkpatrick DK. Don't let your EMR system put you at risk. *AAOS Now*. 2011;5(8). http://www.aaos.org/news/aaosnow/aug11/managing4.asp. Accessed May 9, 2014.
25. The Office of the National Coordinator for Health Information Technology. Guide to privacy and security of health information (version 1.2 060112). 2012. http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf. Accessed May 17, 2014.
26. Thede L. Informatics: electronic health records: a boon or a privacy nightmare? *Online J Issues Nurs*. 2010;15(2).
27. Swift A. Honest and ethics rating of clergy slides to new low. Nurses again top list; lobbyist are worst. 2013. http://www.gallup.com/poll/166298/honesty-ethics-rating-clergy-slides-new-low.aspx. Accessed September 7, 2014.
28. Gaylin DS, Moiduddin A, Mohamoud S, Lundeen K, Kelly J. Public attitudes about health information technology, and its relationship to health care quality, costs, and privacy. *Health Inform Technol*. 2011; 46(3):920–938.
29. Abdel-Monem T, Herian MN, Shank N. Electronic medical records and public perceptions: a deliberative process. *Int J Healthc Inform Syst Inform*. 2013;8(3):38–57.
30. Larsen A. Trappings of technology: casting palliative care nursing as legal relations. *Nurs Inq*. 2011;19(4):334–344.
31. Israel M, Hay I. *Research Ethics for Social Scientists*. Thousand Oaks, CA: Sage Publications; 2006.
32. Lachman VD. Practical use of the nursing Code of Ethics: part II. *Medsurg Nurs*. 2009;18(3):191–194. http://www.nursingworld.org/documentvault/ethics/practical-use-of-the-nursing-code-of-ethics.pdf. Accessed September 7, 2014.

Instructions:
- Read the article. The test for this CE activity can only be taken online at www.nursingcenter.com/ce/CIN. Tests can no longer be mailed or faxed.
- You will need to create (its free!) and login to your personal CE Planner account before taking online tests. Your planner will keep track of all your Lippincott Williams & Wilkins online CE activities for you.
- There is only one correct answer for each question. A passing score for this test is 13 correct answers. If you pass, you can print your certificate of earned contact hours and access the answer key. If you fail, you have the option of taking the test again at no additional cost.
- For questions, contact Lippincott Williams & Wilkins: 1-800-787-8985.

Registration Deadline: February 28, 2017

Disclosure Statement:
The authors have disclosed that they have no financial relationships related to this article.

Provider Accreditation:
Lippincott Williams & Wilkins, publisher of CIN: *Computers, Informatics, Nursing*, will award 2.0 contact hours for this continuing nursing education activity.

Lippincott Williams & Wilkins is accredited as a provider of continuing nursing education by the American Nurses Credentialing Center's Commission on Accreditation.

This activity is also provider approved by the California Board of Registered Nursing, Provider Number CEP 11749 for 2.0 contact hours. Lippincott Williams & Wilkins is also an approved provider of continuing nursing education by the District of Columbia and Florida, CE Broker #50-1223. Your certificate is valid in all states.

Payment:
- The registration fee for this test is $21.95.

For more than 37 additional continuing education articles related to electronic information in nursing, go to NursingCenter.com\CE.

Notice: Online CE Testing Only Coming in 2015!

Starting with the first issue of 2015, the tests for CE articles will appear only in the online version of the issue, and all tests must be completed online at (www.nursingcenter.com/ce/CIN). Simply select the CE article you are interested in. Both the article and the test are available there. You will no longer have the option to mail or fax in the test.
If you haven't done so already, you will want to create a user account for yourself in Nursing Center's CEConnection– it's free to do so! Look for the Login link in the upper right hand corner of the screen.