

EMPLOYEE CONFIDENTIALITY TRAINING FOR THE ELECTRONIC HEALTH RECORD: A SYSTEMATIC REVIEW OF LITERATURE

Posted on December 1, 2015 by Matt

Categories: [2015](#), [EPHIM Archives](#), [Workforce](#)

Abstract

Introduction: The healthcare industry is an ever-changing field, and in recent years, the introduction of the electronic health record (EHR) has enabled hospitals to store and retrieve detailed patient information for use by healthcare providers, and sometimes patients, during a patient's hospitalization, over time, and across care settings. The purpose of this systematic review of literature was to identify the need for healthcare professionals to receive continual and effective training pertaining to the confidentiality of the EHR.

Methods: The systematic review search used three medical-related databases chosen from a university database system to locate articles. The databases used were PubMed, CINAHL Complete, and ProQuest Medical Library. These databases were chosen to gather the suitable references needed to further the research discussion on the topic of electronic health records and confidentiality training.

Results: Fifteen studies covering electronic health records, health information technology, confidentiality, and training were reviewed. The studies assessed the needs of health professionals and health information managers to develop responsibility for confidentiality training and institute more rigorous training on confidentiality.

Conclusion: Training or education of individuals who manage patient health information and its confidentiality is continually needed. Health information managers must address this need and provide training on the policies pertaining to confidentiality. Health information management employees need to have the proper skill set to ensure that patients' personal health information is protected. This review of studies revealed a lack of continued confidentiality training and maintenance among healthcare employees. Healthcare managers need to take more action and be held accountable for training their employees regarding the confidentiality of electronic health records.

Keywords: electronic health records, health information technology, confidentiality, training

Introduction

The healthcare industry is an ever-changing field. In recent years, one of the biggest changes in health information technology (HIT) has been the introduction of the electronic health record. "The electronic health record (EHR) is an electronic record of health related information on an individual that conforms to nationally recognized interoperability standards and that can be managed across more than one healthcare organization."¹ One of the main concerns with the EHR is confidentiality of

the record. Many people do not trust that the technology is secure enough to store and track this sensitive information. "Research shows that individuals support the use of technology to improve the health care system but despite government focus on protections, they remain concerned about privacy and security of their health information."² Health professionals need to be educated on how to use this technology effectively while keeping patient information confidential. The gaps in the education and training of healthcare professionals are an issue that needs to be addressed. According to Goodman, "Failure to provide adequate training in health information technology will impede the evolution of HIT as a public health resource."³ Confidentiality of health information includes not only protecting patient information on the employee side but also allowing patients to have ease of access to their health resources.

The EHR is the future of the healthcare industry. Ideally, the EHR would be available regardless of where an individual decides to go for healthcare services. The main issue at this point is that many patients do not trust the system. Training employees to use this technology to protect information and also teaching them how to talk to patients about the benefits and safety of the EHR is essential. The dynamic of the patient-physician relationship is shifting. With the increase in technology, patients have a desire to contact their physicians using new methods. "Previous studies have reported that 90% of patients with Internet access would like to contact . . . their physician regarding administrative issues, medication concerns and other aspects of care."⁴ Because providers and patients are increasingly leaning toward a more technology-driven healthcare experience, having employees trained in the proper methods of ensuring confidentiality of health information is vital not only for protection of that information, but also to ensure that patients feel the information is safe, which lets them trust the EHR. To help determine if employees are receiving enough confidentiality training with the EHR, the development of surveys is needed to help gauge where the current needs lie. According to Hersh, quoted by Fenton et al., "We have little data that characterizes the HIT workforce and, in particular, how it is best trained and deployed for optimal use of the technology."^{5, 6}

This systematic review is aimed at identifying healthcare professionals' need to receive effective training in keeping patient information confidential through the EHR, and how this training can be used to make patient care a more collaborative effort.

Methods

Three medical-related databases within a university database system were used to locate articles. The databases were PubMed, CINAHL Complete, and ProQuest Medical Library. These databases were chosen to gather suitable references to further the research discussion on the topic of HIT and confidentiality.

The CINAHL Complete database was used to conduct two searches, resulting in a total of five

articles. The advanced search function in CINAHL Complete was used to conduct a more specific article search. The key phrase "health information technology" was entered in the main search field, and the Boolean "AND" function was used to include the keyword "confidentiality." The search yielded 461 peer-reviewed article results. The full-text option was selected, narrowing the search to 195 peer-reviewed articles. The publication date range was set to 2010 through 2015, which yielded 91 articles. Of these 91 articles, the best three articles that would provide supporting research were chosen. To find more articles, another search was conducted using the CINAHL Complete database with different keywords. The advanced search function was used again. The key phrase "electronic health records" was used in the main search box this time, and the Boolean function "AND" was used to include the keyword "confidentiality." This search yielded 494 article results. To narrow this article search, full-text availability and a publication date range of 2010 through 2015 were used as criteria. These criteria narrowed the results to 113 peer-reviewed articles. Two of those articles were chosen for the research topic.

The PubMed database was used similarly to CINAHL. Entering "health information technology and confidentiality" in the search field and narrowing down the articles to those published within the past five years and available in full text resulted in 914 peer-reviewed articles. Three articles that would be helpful to the research were found in this search. Two more peer-reviewed articles were found in PubMed by searching for "electronic medical records and patient privacy." Setting the publication dates to within five years reduced the number of results from 1,493 to 738.

ProQuest Medical Library was the last database used. The search started with "electronic health record and (patient-provider) and communication" and was filtered to include only scholarly journals, peer-reviewed articles, and articles published in the last five years, resulting in 542 articles. When the Boolean function "AND" and the word "confidentiality" were added, the search resulted in 103 articles. From these results, five articles were selected on the basis of their relevance to this topic.

Results

The articles reviewed in this systematic review of literature address the issues of confidentiality training among employees in healthcare settings. The articles also discuss the importance of patient involvement in the use of EHRs and the dialogue that providers need to start with their patients discussing the benefits of the EHR. The remaining articles discuss whether patients trust the use of the EHR and what providers can do to gain or ruin this trust.

The five articles that discuss confidentiality training among employees had a common theme of the need for more education or continuing education. The studies are summarized in [Table 1](#). Fenton et al. conducted 12 focus groups, with 9 of the 12 groups spread throughout the state of Texas and the remaining three groups held as web conferences.⁷ In that study, current HIT employees were asked

to help identify skills necessary to maintain confidentiality in health records and to help determine if more needs to be done to educate employees in dealing with confidentiality of records. These skills were broken into three categories: basic, intermediate, and advanced. Fenton et al. identified basic skills as including basic computer skills and Internet skills. These basic skills were identified as an important educational tool for maintaining confidentiality. In the intermediate skills category, Fenton et al. identified knowledge of HIPAA, knowledge of privacy regulations, and data sharing skills as important educational tools for confidentiality. In the final category of advanced skills, Fenton et al. identified the management skills of staff in relation to EHR systems as an important educational tool.⁸ In another study, conducted by Baskaran et al., 24 questionnaires were completed out of 52 that were sent to various healthcare settings.⁹ Baskaran et al. found that 75 percent of the healthcare employees surveyed had received some type of training or education regarding security and rights to access patient information. However, they also found that more than 80 percent of those surveyed had shared the password that allowed access to sensitive patient information.¹⁰

The studies of Koontz¹¹ and Wikina¹² did not make use of a questionnaire or survey, but in these studies researchers discovered a lack of education among employees regarding confidentiality standards and maintenance. The authors of an American Health Information Management Association (AHIMA) guide stated that education is necessary to prevent confidentiality breaches. The researchers mentioned that new employees need training focused on setting expectations and practices regarding access to EHRs and policies relating to EHRs.¹³ They also mentioned that current employees should be given a refresher course in confidentiality yearly.¹⁴ Koontz states that leadership of managers is key in confidentiality practices.¹⁵ Simple steps can be taught to help with confidentiality of EHRs. These steps include strong passwords that are not shared, physical security in the office space, complete annual Health Insurance Portability and Accountability Act (HIPAA) training, continued training of employees regarding federal and state laws, and the realization that the healthcare industry is not static and will continuously change. To support this trend, the Wikina study reports that four key "pillars" lead to effective confidentiality practices among employees.¹⁶ The first pillar mentioned by Wikina is leadership, the second pillar is awareness and continuing education, the third pillar is managers' actions, and the final pillar in creating strong confidentiality is monitoring and evaluating.¹⁷

The literature supports the movement toward an electronic platform (see [Table 2](#)). Esquivel et al. address the recommendation to make EHR communication more efficient in the use of referrals. The authors discuss ways to make the process more efficient; however, one of the main points is to minimize the sharing of unnecessary information by having policies and procedures in place to guide physicians regarding what information is necessary to be shared.¹⁸ To further support this

point, Peck addresses the effective use of the EHR in patient communication.¹⁹ She calls for more training for both doctors and students in using the EHR with patients in communication and face-to-face interactions.²⁰ Professionals need training on how to interact with patients when using the electronic platform.

In a point-and-counterpoint article, Caine and Tierney examine the issue of physician access to patient records.²¹ Caine makes the point that having access to the whole record at the time the physician sees a patient would lead to more efficient care. Tierney makes the point, however, that while such access would be helpful, not all doctors need to see all of a patient's medical information. He proposes that patients should have the power to choose the information they allow their doctors to see.²²

Mandl brings up the point that patients are concerned with the privacy of their records, calls for interoperability within the systems being used, and suggests that patients have the final say in who sees their records. The medical record should be accessible but still kept private. It is important that doctors understand that patients are becoming more hands-on in their medical care and that the EHR is making it possible for patients and doctors to collaborate. Training needs to be provided so that doctors know how to work with patients this way.²³

A study by Maiorana et al. examined confidentiality in health information exchanges in relation to patients with HIV. The main finding of the study relates to the patients' comfort level in sharing their information on these portals because they realize the trend of healthcare. Patients and doctors need to be comfortable with these platforms, and the best way to make everyone comfortable is to provide more training. As patient trust begins to grow, it is important that doctors be able to keep the trust and not ruin it by breaching confidentiality.²⁴

In "Anonymising and Sharing Individual Patient Data" by El Emam et al., data sharing is categorized into three types: public data, quasi-public data, and nonpublic data. The types depend on how easily accessible the data are. Simple changes to the data being used in research substantially reduce the probability of re-identification. In this article, the authors discuss methods that can be used to measure the risk of re-identification based on what type of data category is being used and thereby make the data anonymous at a certain level.²⁵

The study by Meystre et al. makes a great point regarding how certain data affect the physician's standpoint when given de-identified patient information. When physicians were asked to try to re-identify specific de-identified patients based on their discharge summary, none of the 86 patients were correctly identified. The physicians involved in the study were confident that they would be able to recognize the patient on the basis of specific clinical information, but this study proved them

to be wrong. This study shows that de-identification may help in the area of patient confidentiality.²⁶

As healthcare switches from paper records to EHRs, every job in the healthcare field will require the use of a computer. In "Ethical Issues in Electronic Health Records: A General Overview," Ozair et al. found that the keys to finding solutions are leadership, teamwork, flexibility, and adaptability. To obtain the benefits that EHRs will offer, risks will need to be recognized and either properly managed or overcome.²⁷

In the study conducted by Patel et al., positive healthcare experiences and higher information efficacy were associated with more favorable perceptions of privacy and security. These authors found that 12.33 percent of participants withheld important information from their provider because of privacy and security concerns regarding their medical information. This study shows that a higher quality of care and patient satisfaction will result in more confidence and trust in patient information.²⁸

The article by Williams et al. talks about how important patient and public trust is in the area of medical research and how easily this trust may be threatened. Williams et al. propose a dynamic consent model that provides a transparent, flexible, and user-friendly means to maintain public trust by allowing patients to control consent electronically throughout time and receive information dealing with the use of their personal data. Dynamic consents provide a platform to develop the ethical and engagement framework to ensure respect for the rights, needs, and expectations of diverse participants while widening participation and maintaining trust.²⁹ Studies addressing patient trust in the confidentiality of information are summarized in [Table 3](#).

Discussion

The five key studies addressing confidentiality all support the notion that confidentiality training is a missing component of healthcare. The studies reveal a number of educational tools that can be used to instruct healthcare employees regarding confidentiality. However, most facilities currently have no standard, mandated yearly training for employees on confidentiality. This review of studies suggests that employees know what they should and should not be doing regarding confidentiality but still commit errors in confidentiality practices. The evidence in these studies indicates a need to provide universal education for healthcare employees with annual training to improve the confidentiality of EHRs and to reduce complacency or lack of knowledge.

Annual confidentiality training modules are needed throughout healthcare facilities to maximize the security and confidentiality of patient information in the EHR. Although employees go through initial training covering confidentiality upon being hired, further education is needed on topics such as how to discuss confidentiality, electronic security, and doctor-patient communication.

The apathetic attitude toward patient confidentiality in the EHR needs to be addressed. Health providers need to be more intentionally aware of sensitive patient information. Providers and employees know how confidentiality should be maintained but choose not to act, and this situation needs to change in order for the transition to a mostly or fully electronic record system to be successful. Reinforcement of confidentiality training among healthcare employees is insufficient. With the rise of communication through EHR platforms, this need is more crucial than ever.

Conclusion

This review of studies revealed a lack of confidentiality training and maintenance among healthcare employees. Healthcare managers need to take more action and be held accountable for training employees in the confidentiality of EHRs. With the transition from paper to electronic records, holding annual training sessions in the healthcare setting is more important than ever. It is essential for patients to feel confident about the security of their personal health information. For the implementation of EHRs to be successful, patients need reassurance from their providers that their information is safe and confidential. Through increased initiatives in the training of healthcare employees, patients can be afforded confidence in the confidentiality of information.

Julia VanderMolen, PhD, is an assistant professor of allied health sciences at Grand Valley State University in Grand Rapids, MI.

Alesha Prince is a student at Grand Valley State University in Allendale, MI.

Emily Neu is a student at Grand Valley State University in Allendale, MI.

Rachael DeKraker is a student at Grand Valley State University in Allendale, MI.

Notes

1. Sayles, Nanette. *Health Information Management Technology: An Applied Approach*. 4th ed. Chicago: AHIMA Press, 2013.
2. Koontz, Linda. "Health Information Privacy in a Changing Landscape." *Generations* 39, no. 1 (2015): 97–104.
3. Goodman, K. W. "Ethics, Information Technology, and Public Health: New Challenges for the Clinician-Patient Relationship." *Journal of Law, Medicine & Ethics* 38, no. 1 (2010): 58–63.
4. Solera Ruiz, Irene, Guadalupe Poblaciòn García, and Irene Riquelme. "E-mail Communication in Pain Practice: The Importance of Being Earnest." *Saudi Journal of Anaesthesia* 8, no. 3 (2014): 364–67.
5. Hersh, W. "The Health Information Technology Workforce: Estimations of Demands and a

- Framework for Requirements." *Applied Clinical Informatics* 1, no. 2 (2010): 197–212.
6. Fenton, Susan H., Elizabeth Joost, Jimena Gongora, Davis G. Patterson, Holly A. Andrilla, and Susan M. Skillman. "Health Information Technology Employer Needs Survey: An Assessment Instrument for Workforce Planning." *Educational Perspectives in Health Informatics and Information Management* (Winter 2013).
 7. Ibid.
 8. Ibid.
 9. Baskaran, Vikraman, Kim Davis, Rajeev K. Bali, Raouf N. G. Naguib, and Nilmini Wickramasinghe. "Managing Information and Knowledge within Maternity Services: Privacy and Consent Issues." *Informatics for Health & Social Care* 38, no. 3 (2013): 196–210.
 10. Ibid.
 11. Koontz, Linda. "Health Information Privacy in a Changing Landscape."
 12. Wikina, Suanu Bliss. "What Caused the Breach? An Examination of Use of Information Technology and Health Data Breaches." *Perspectives in Health Information Management* (Fall 2014).
 13. Walsh, T., and W. Miaoulis. "Privacy and Security Audits of Electronic Health Information." *Journal of AHIMA* 88, no. 3 (2014): 54–59.
 14. Ibid.
 15. Koontz, Linda. "Health Information Privacy in a Changing Landscape."
 16. Wikina, Suanu Bliss. "What Caused the Breach? An Examination of Use of Information Technology and Health Data Breaches."
 17. Ibid.
 18. Esquivel, Adol, Dean F. Sittig, Daniel R. Murphy, and Hardeep Singh. "Improving the Effectiveness of Electronic Health Record-based Referral Processes." *BMC Medical Informatics and Decision Making* 12 (2012): 107.
 19. Peck, Andrea Downing. "Making the EHR Your Partner in Patient Care." *Medical Economics* 90, no. 18 (2013): 50–53.
 20. Ibid.
 21. Caine, Kelly, and William M. Tierney. 2015. "Point and Counterpoint: Patient Control of Access to Data in Their Electronic Health Records." *Journal of General Internal Medicine* 30, suppl. 1 (2015): S38–S41.
 22. Ibid.
 23. Mandl, K. D. "Public Standards and Patients' Control: How to Keep Electronic Medical Records Accessible But Private." *British Medical Journal* 322 (2001): 283.
 24. Maiorana, Andre, Wayne T. Steward, Kimberly A. Koester, Charles Pearson, Starley B. Shade, Deepalika Chakravarty, and Janet J. Myers. "Trust, Confidentiality, and the Acceptability of Sharing HIV-related Patient Data: Lessons Learned from a Mixed Methods Study about Health Information Exchanges." *Implementation Science* 7 (2012): 34.
 25. El Emam, Khaled, Sam Rodgers, and Bradley Malin. 2015. "Anonymising and Sharing Individual

- Patient Data." *BMJ* 350 (2015): h1139.
26. Meystre, Stéphane, Shuying Shen, Deborah Hofmann, and Adi Gundlapalli. "Can Physicians Recognize Their Own Patients in De-identified Notes?" *Studies in Health Technology and Informatics* 205 (2014): 778–82.
 27. Ozair, Fouzia F., Nayer Jamshed, Amit Sharma, and Praveen Aggarwal. "Ethical Issues in Electronic Health Records: A General Overview." *Perspectives in Clinical Research* 6, no. 2 (2015): 73–76.
 28. Patel, Vaishali, Ellen Beckjord, Richard P. Moser, Penelope Hughes, and Bradford W. Hesse. "The Role of Health Care Experience and Consumer Information Efficacy in Shaping Privacy and Security Perceptions of Medical Records: National Consumer Survey Results." *JMIR Medical Informatics* 3, no. 2 (2015): E14.
 29. Williams, Hawys, Karen Spencer, Caroline Sanders, David Lund, Edgar A. Whitley, Jane Kaye, and William G. Dixon. "Dynamic Consent: A Possible Solution to Improve Patient Confidence and Trust in How Electronic Patient Records Are Used in Medical Research." *JMIR Medical Informatics* 3, no. 1 (2015): E3.

[Printer friendly version of this article.](#)

There are no comments yet.