

Patients and Health Care Providers' Concerns about the Privacy of Electronic Health Records: A Review of the Literature

Nicola T. Shaw¹, Anjali Kulkarni², Rebecca L. Mador²

¹Health Informatics Institute, Algoma University, Sault Ste. Marie, ON, Canada

²Faculty of Medicine & Dentistry, University of Alberta, Edmonton, AB, Canada

Abstract

Electronic Health Records hold the potential for great improvements in healthcare provision yet take-up in North America remains slow behind Australia and Europe. We believe that one of the reasons for this is the lack of attention to privacy concerns. A structured literature review was undertaken to identify the current state of knowledge concerning patients and Health Care Provider's (HCP) perspectives on privacy and the EHR. Twenty-one papers were ultimately identified and are discussed here. Two main themes were identified: General concerns with the privacy of EHRs and specific concerns regarding sharing information within EHRs. Based on the literature reviewed, and acknowledging the limitations of the literature in this field, it would appear that in general patients were less concerned with the privacy of their personal health information within EHRs than their HCPs were. If this is indeed the case, this leaves an interesting conundrum for us to consider: Do we have a duty to protect patients, even from themselves, with regards to the sharing of their personal health information?

Keywords: *Electronic Health Records, Privacy*

1. Introduction

Electronic Health Records (EHR) provide a single shared resource for the collection, storage, and use of patient data by health care providers [1]. They are believed to increase the quality of patient care by facilitating access to information, improving communication, and providing clinical decision support [2]. However, concerns have been raised regarding the privacy of personal health information contained in EHRs [3, 4].

Indeed, there have been several high profile stories in the media detailing breaches of private patient health information [5]. Recent polls have found that almost nine million Americans believe that their health information has been either lost or stolen [6] while another survey found that American physicians have so little trust in their government's use of the information stored in EHRs, that they would rather retire than adopt these electronic systems [7]. Given these figures, it is not surprising that the rate of

EHR adoption in Canada and the United States has been advancing at a snail's pace.

To date, little attention has been paid to clarifying the concerns associated with the privacy of EHRs, as perceived by patients and Health Care Providers (HCP). However, left undefined and unresolved, these issues may significantly affect the quality of EHRs, the speed at which they are implemented, the speed with which they are adopted and taken up by consumers and providers, the ability to exchange health information between institutions and, ultimately, the quality of patient care and patient safety.

Therefore, the purpose of this review was to answer the question: ***“Are health care providers and patients concerned about the privacy issues associated with EHRs?”*** with the intent of using the findings to inform the development of a substantial survey of providers and patients to be conducted in 2010/2011. The proposed future research will concentrate on developing a greater understanding of what

providers and consumers expect in terms of the privacy of EHRs and exploring the conundrum identified in this structured review.

2. Methods

Systematic searches were conducted between May 2008 and June 2008 on PubMed Central, EMBASE, CINAHL, Cochrane Library, IEEE Xplore, Patient Safety Resource Guide, and the Canadian Medical Association CPG InfoBase.

Because there is no single industry-wide accepted definition of what constitutes an EHR we used Canada Health Infoway's [8] definition for the purpose of this review. Infoway defines an EHR as *"a secure and private lifetime record of an individual's health and care history, available electronically to authorized health care providers"* [8]. Moreover, we defined a HCP as *"a person who helps to identify, prevent, or treat an illness or disability"* [9]. We chose this definition because it is broad and includes professionals from allied health disciplines as well more traditional HCPs, such as physicians and nurses. We felt that it was important to include the perspectives of as many disciplines as possible because, as EHRs become more widely adopted and interoperable, the number of HCPs who could have electronic access to patients' health information will expand dramatically.

In the context of EHRs, privacy refers to the ability to control or limit access to one's personal health information [10]. However, other terms, such as security and confidentiality, are often used interchangeably with privacy [10]. While these three concepts are distinct, they are inextricably linked and, to the best of our knowledge, have not been well defined or studied individually within the context of EHRs. For this reason, we have chosen to define privacy broadly and include a wide range of data on this topic, regardless of whether it has been labeled as a privacy, confidentiality, or security issue.

2.1 Selection Criteria

In order to be included in this review, articles had to discuss privacy issues associated with EHRs, and be published in the English language or have an accessible English-language translation available. Articles also had to report on the perspectives of HCPs (as defined above) and/or patients (adult or pediatric), and provide original experimental data. Because the use of EHRs is relatively new, we did not place a limit on the publication date of the articles included. However, articles were excluded if they discussed privacy issues associated with pharmacies, research subjects; the use of e-mail communication; concerns other than those associated with privacy; and, were opinion-based articles that did not produce original research to buttress their conclusions.

2.2 Data Extraction & Quality Assessment

Articles that met the inclusion criteria were then read in order to confirm inclusion and to extract relevant methodological details including: the study's objective or hypothesis, design, participant demographic details, location of study, as well as the study's main results and conclusions. We adapted criteria that had previously been developed by Petticrew and Roberts [11] and Khan et al [12] in order to assess the methodological quality of the quantitative studies. These criteria reflect the importance of ensuring a high degree of internal and external validity in published research. Qualitative studies were evaluated based on criteria published by Petticrew and Roberts [11] and by Spencer et al [13].

2.3 Data Analysis

Because the studies were so varied in terms of the design, context, and participants, a formal meta-analysis was deemed to be inappropriate. Rather, we decided to extract the main findings related to the privacy of EHRs and analyze the content thematically. Two of the authors (RLM & AK) independently read the included articles and identified the passages relating to key issues from our research questions. The senior author (NS) then read the identified articles and conducted an independent analysis in order to triangulate our results. The results of both sets of analysis were then combined and are presented here. Two major themes emerged: general concerns with the privacy of EHRs; and, sharing information contained within EHRs.

3. Results

Extensive searches found twenty-one articles [3; 10; 14-31] that met our inclusion criteria. The studies represented a cross-section of countries and, consequently, political climates and EHR adoption histories. Of the final twenty-one studies included in this literature review, nine were from the USA [10;15;16;18;21;22;24;32], five were from the UK [19;27-30], two were from New Zealand [3;20], and one study from each of Ireland [23], Canada [25], Norway [26], Denmark [31], and Oman [17] (located in the Middle East). Fourteen studies were quantitative [3; 10; 14; 16-25; 33] and used cross-sectional baseline surveys and questionnaires to collect data. Seven were qualitative designs [26-32], which employed focus groups and interviews. Not surprisingly, the studies were all published within the last 14 years (1994 – 2008).

Only six studies [3; 10; 19; 22; 23; 25] investigated the concerns associated with privacy and EHRs as a main objective. The other studies investigated general concerns associated with EHRs, with privacy being a minor component or having arisen spontaneously through related ques-

tioning. Five studies [17; 18; 21; 23; 24] investigated health care providers' concerns, Fourteen [3; 10; 14; 16; 19; 20; 22; 25-31] provided insight into patients' concerns, while only one study [15] investigated both groups' concerns. Although we defined HCPs broadly physicians and nurses were almost always the targeted HCP group. Only one study [32] obtained data from other types of hospital staff (e.g. registered nurses, licensed vocational nurses, nursing assistants, unit clerical staff, a clinical nurse specialist and managers).

3.1 General Concerns with the Privacy of EHRs

Fourteen studies [3;14-16;21;22;24;25;27-32] reported on general concerns associated with the privacy of personal health information contained in electronic form. Hassol et al. [22] found that the majority of their patient population had little or no concern about the privacy of EHRs. Similarly, Honeyman et al. [29] reported that 77% of their patient respondents were not concerned either. In contrast to their findings was a study by Flynn et al. [14], which found that the vast majority of their psychiatric patient population was very concerned about the privacy of their personal health information stored on EHRs. It should also be noted that almost all studies reported a subset of patients who had "serious" concerns regarding the privacy of information. For example, 27% of Californians and 30% of patients who used a patient portal were concerned about the privacy of their information [16].

HCPs, on the other hand, were found to be more concerned than the patient respondents about privacy. In one study [24], the researchers found that nearly 50% of staff believed that an EHR would result in increased risks to patient confidentiality.

Across groups, there was a significant amount of concern about the possibility of unauthorized access from within, and outside of, the health care system. Three papers [3; 21; 31] reported that both patients and HCPs were worried about the potential for hackers to enter a computerized system. Several studies (e.g. [27]) found that patients were afraid that non-medical individuals (such as insurance companies, lawyers and other patients) may gain access to their files or may accidentally see their record. Of note, patients were especially worried that individuals might gain access to their mental or sexual health information [28] and some hospital staff were concerned that computer use would result in increased surveillance by government agencies [24].

Four studies [14; 25; 27; 28] reported patient fears about the consequence of unauthorized access. One study [14], which investigated the specific fears of psychiatric patients, found that these patients were concerned that they would be stigmatized as a result of their mental illness if their record was accessed inappropriately. Other studies found that patients were concerned about the commercial use and exploitation of their information [27] and that their

health information would be used for spiteful reasons including blackmail and gossip [21; 28].

3.2 Sharing Information in EHRs

The second major theme that emerged from our review of the literature related to how, with whom, and in what contexts participants believed that electronic health information should be shared. The authors of these studies found that patients were not comfortable sharing their medical information in its entirety and believed that some limitations should be put in place [23]. However, there was no discussion about what limitations these should be. Results were mixed with respect to which information patients believed should be withheld, with patients becoming more unwilling to have their information released, the more personal it was [10]. Patients were most unwilling to share information related to their sexual and mental health [27]. All respondents believed that patient consent should be obtained prior to sharing any health information (e.g. [20]).

The identity of the individuals with whom information could be shared was a contentious issue. While there was consensus among both patient and HCP respondents that health information on EHRs should be shared with other providers, there was no clear consensus on which HCPs should be privy to this information. For example, two studies [27;31] found that both physicians and patients believed that medical information should be shared with all health care providers, while in another study [20] many patients felt that only physicians and other HCPs that have been specifically identified should have access to their information. This group was also against having their information shared with private health insurers or with government agencies.

Interestingly, a theme that emerged spontaneously in three studies [10; 25; 30] was that of trust in the custodians of EHRs. Though one study [10] reported that the majority of patients had a high level of trust in how their information was being shared, two other studies [25; 30] reported that their respondents felt that information was not being adequately protected. Interestingly, the highest reported level of trust was in primary health care professionals with the least amount of trust being had for those outside the health provider circle, such as researchers.

4. Discussion

There is a limited amount of research that has investigated the concerns of patients and HCPs with respect to the privacy of health information stored on electronic systems. Interestingly, this review found that patients are much less concerned with the privacy of their personal information than their HCPs are. This is in contrast to recent polls [6;7] conducted in the US that have indicated

that privacy is a significant issue for individuals and a barrier to large scale implementation of these systems.

Not surprisingly, patients who have experienced stigmatization because of a health issue have significant concerns with respect to the privacy of their information. This area must be investigated further, as the implications for patient safety and care are immense. If patients are worried about their personal privacy, they may fail to disclose important information to their HCPs, which will ultimately hinder the care that they receive. This may be an even more critical issue for vulnerable populations who are already distrustful of health care institutions.

This review found a number of areas of concern for patients with respect to how their information is shared. Patients did not want information shared indiscriminately, yet there was no clear consensus on how the sharing of information should be managed. HCPs were among the strongest opponents of sharing their patients' health information without prior consent, yet they believed that other health care providers should have access to this information. There is a clear need to balance these two differing perspectives. Much more research is needed to clarify these issues and to identify whether or not a compromise can be reached; one that allows HCPs to feel confident that they have access to the information they need whilst also ensuring that their patients' information and their right to privacy is protected.

5. Strengths and Weaknesses of the Available Evidence

Importantly, these studies may not be generalizable to other sub-patient populations or from country to country where legislation to protect private health information varies. Furthermore, the financial model in different countries may have a strong impact on perspectives depending on whether or not there is a relationship between payer and funder.

None of the studies focused on HCPs concerns with whether they feel that they have the necessary tools or knowledge to maintain their patients' information in a safe and secure manner, nor at the costs associated with doing so. Similarly, none of the studies distinguished between the various different definitions of security, privacy, and confidentiality, yet these are distinct concepts. For example, confidentiality refers to information that is kept secret by the HCP to whom it is disclosed, whereas security refers to the things that are put in place in order to maintain a patient's right to privacy. None of the studies included in our sample distinguished between these varying concepts, yet this may have had a significant impact on how a participant responded.

6. Conclusion

In conclusion, both HCPs and patients are concerned about the privacy issues associated with EHRs, though patients seem to be somewhat less concerned than HCPs. However, both groups recognize that the sharing of personal health information electronically through such mechanisms as EHRs is inevitable at this point. Yet despite this, much remains to be answered as to what information should be shared with whom and when. In today's high-tech world, where a growing number of adolescents and adults share their personal information on websites, such as Facebook, these issues are fast becoming ubiquitous. Websites like GoogleHealth may effectively desensitize individuals, lulling them into a false belief in the privacy of these programs. Consequently they may simply not realize the potential consequences of allowing their personal health information to be freely shared. The question then becomes: *do we as professionals have a duty to protect patients even from themselves?* Answering this question will be the focus of the next stage of this study which will take the form of a substantial survey of providers and patients to be conducted in 2010/2011.

References

1. Sujansky WV. The benefits and challenges of an electronic medical record: much more than a "word-processed" patient chart. *West J Med* 1998; 169(3):176-183.
2. Cusack CM. Electronic health records and electronic prescribing: Promises and pitfalls. *Obstetrics and Gynecology Clinics of North America*. 35[1], 63-79. 2008.
3. Chhanabhai P, Holt A. Consumers are ready to accept the transition online and electronic medical records if they can be assured of the security measures. *Medscape General Medicine* 9[1]. 2007.
4. Pendrak RF, Ericson RP. Information technologies need to protect patient confidentiality. *Healthc Financ Manage* 1998; 52(10):66-68.
5. David R. Records safe with us, says NHS chief. *The Times*. 2007.
6. The Harris Poll #74. Millions believe personal health information has been lost or stolen. *The Harris Poll #74* [2008 [cited 2009 Mar. 13]; Available from: URL:http://www.harrisinteractive.com/harris_poll/index.asp?PID=930
7. Manos D. Survey shows doctors don't trust the government's use of EHRs. *Healthcare IT News* [2008 [cited 2009 Mar. 13]; Available from: URL:<http://www.healthcareitnews.com/news/survey-shows-doctors-dont-trust-governments-use-ehrs>
8. Canada Health Infoway. Canada Health Infoway. Canada Health Infoway [2005 [cited 2007 Jan. 22]; Available from: URL <https://www.infoway-inforoute.ca/lang-en>
9. The Canadian Oxford Paperback Dictionary. Don Mills, ON: Oxford University Press Canada; 2000.

10. Goodwin L, Courtney K, Kirby D, Iannacchione MA. A pilot study: Patients' perceptions about the privacy of their medical records. *Online Journal of Nursing Informatics* 6[3 [on-line]], Online. 2002.
11. Petticrew M, Roberts H. *Systematic Reviews in the Social Sciences: A Practical Guide*. Blackwell Publishing; 2006.
12. Khan K, Ter Riet G, Popay J, Nixon J, Kleijnen J. Study quality assessment - phase 5.
13. Spencer L, Ritchie J, Lewis J, Dillon L. Quality in qualitative evaluation: A framework for assessing research evidence.
14. Flynn H, Marcus S, Kerber K, Alessi N. Patients' concerns about and perceptions of electronic psychiatric records. *Psychiatric Services* 54[11], 1539-1541. 2003.
15. Gadd C, Penrod L. Dichotomy between physicians' attitudes regarding EMR use during outpatient encounters. *Proceedings / AMIA Symposium*, 275-279. 2000.
16. Pennbridge J, Moya R, Roderigues L. Questionnaire survey of California consumers' use and rating of sources of health care information including the internet. *Western Journal of Medicine* 171, 302-306. 1999.
17. Al Farsi M, West D. Use of electronic medical records in Oman and physician satisfaction. *Journal of Medical Systems* 30[1], 17-22. 2006.
18. Russell S. Barriers to EMR adoption in internal medicine and pediatric outpatient clinics. *Tennessee Medicine* 97[10], 457-460. 2004.
19. Powell J, Fitton R, Fitton C. Sharing electronic health records: the patient view. *Inform Prim Care* 2006; 14(1):55-57.
20. Whiddett R, Hunter I, Engelbrecht J, Handy J. Patients' attitudes towards sharing their health information. *Int J Med Inform* 2006; 75(7):530-541.
21. Likourezos A, Chalfin D, Murphy D, Sommer B, Darcy K, Davidson S. Physician and nurse satisfaction with an electronic medical record system. *Computers in Emergency Medicine* 27[4], 419-424. 2004.
22. Hassol A, Walker JM, Kidder D, Rokita K, Young D, Pierdon S et al. Patient experiences and attitudes about access to a patient electronic health care record and linked web messaging. *J Am Med Inform Assoc* 2004; 11(6):505-513.
23. Feeney L, Moran P. Information sharing and risk: A survey of psychiatrists. *Irish Journal of Psychological Medicine* 24[3], 94-98. 2007.
24. McLane S. Designing an EMR planning process based on staff attitudes toward and opinions about computers in health-care. *Computers Informatics - Nursing* 23[2], 85-92. 2005.
25. Lysk M, Roch J. Electronic health information and privacy survey: What Canadians think-2007. *Canada Health Infoway*. 2008.
26. Tjora A, Tran T, Faxvaag A. Privacy vs usability: A qualitative exploration of patients experiences with secure internet communication with their general practitioner. *Journal of Medical Internet Research* 7[2]. 2005.
27. Pyper C, Amery J, Watson M, Crook C. Patients' experiences when accessing their on-line electronic patient records in primary care. *Br J Gen Pract* 2004; 54(498):38-43.
28. Risdale L, Hudd S. Computers in consultation: The patient's view. *British Journal of General Practice* 44, 367-369. 1994.
29. Honeyman A, Cox B, Fisher B. Potential impacts of patient access to their electronic care records. *Informatics in Primary Care* 2005; 13(1):55-60.
30. Tracy S, Dantas G, Upshur REG. Feasibility of patient decision aid regarding disclosure of personal health information: Qualitative evaluation of the Health Care Information Directive. *BMC Medical Informatics & Decision Making* 4[13]. 2004.
31. Zuirita L, Nohr C. Patient opinion - EHR assessment from the users' perspective. *Medinfo* 2008 11, 1333-1336. 2008.
32. Zandieh S, Yoon-Flannery K, Kuperman GJ, Langsam D, Hyman D, Kaushal R. Challenges to EHR implementation in electronic versus paper-based office practices. *Journal of General Internal Medicine* 23[6], 755-761. 2008.
33. Gadd CS, Penrod LE. Assessing physician attitudes regarding use of an outpatient EMR: a longitudinal, multi-practice study. *Proc AMIA Symp* 2001; 194-198.

Correspondence

Dr. Nicola Shaw, FBCS, CITP
ESRI Canada Health Informatics Research Chair & Health Informatics
Institute Scientific Director
Room SH500
Health Informatics Institute
Algoma University
1520 Queen Street East
Sault Ste. Marie
Ontario
P6A 2G4
Canada

Tel: +1 705 949 2301 x4751
Fax: +1 705 946 7361
Email: nicola.shaw@algonau.ca