SciMedCentral

Annals of Nursing and Practice

Review Article

Privacy Issues with the Electronic Medical Record

Pamela J Aselton* and Sandra Affenito

Nursing Department, School of Health and Natural Sciences, University of Saint Joseph, USA

***Corresponding author**

Aselton, Pamela J, Nursing Department, Interdisciplinary faculty, USA, Email: paselton@nursing.umass.edu

Submitted: 15 July 2014

Accepted: 27 September 2014

Published: 29 September 2014

Keywords

- Electronic medical record
- Privacy issues
- EMR- electronic medical record

Abstract

Electronic medical records (EMR) all have privacy safeguards in place. Major healthcare institutions have taken steps to prevent employees from looking up information on patients whom they do not treat directly, however numerous potential intrusions into patient privacy are still possible. Centralization of medical records in the increasing number of multi-group practices distributes personal medical data over larger networks and increases the likelihood that personal medical data may be shared or viewed by unauthorized users. This article reviews the benefits of EMRs and the possible mechanisms by which data may be shared without patient knowledge, as well as solutions and safeguards that need to be taken to protect the privacy of patient medical records.

INTRODUCTION

The Patient centered Medical Home (PCNH) or medical home is a redesign of primary care. The PCMH provides coordinated care, allowing for more appropriate use of resources, resulting in enhanced patient care outcomes and reduced costs [1]. The National Committee for Quality Assurance aims to ensure primary care practitioners meet the following six standards, which include: (1) enhance access and continuity; (2) identify and manage patient populations; (3) plan and mange care; (4) provide self care and community support; (5) track and coordinate care and (6) measure and improve performance [2]. There is a growing body of literature which supports the use of electronic medical records(EMRs) as being essential to meet these indicators of quality of care [3].

Government incentives, ease of billing, and the promise of increased patient safety and convenience for healthcare providers across all professions have been the rationales for the widespread adoption of the electronic medical record. Electronic medical records(EMRs) are more efficient compared with paper records and are thought to improve the quality and safety of the care patients receive both in hospital settings and outpatient clinics by making patient data more readily available to providers (Freudenheim, 10/8/12). In addition, EMRs enable clinicians to share information, target clinical decision support, communicate health care team information with patients and access all providers' documentation and patient's medical tests.

Stage II of the 2009 American Recovery and Reinvestment Act is intended to be enacted in during the 2013 to 2014 period and requires EMRs to have a list of care team members available for at least 10% of patients [2]. However, with the increased commercial gathering of personal data online to distribute to interested parties, the potential of wholesale distribution of personal medical information is a possible confidentiality issue with this technology. The Health Insurance Portability and Accountability Act 1996 (Public Law 104-191 (HIPPA) has established a set of regulations to standardize collection as well as the storage and dissemination of individually identifiable health information. This act required consistent codes and identifiers for each provider with the aim to have all Medicare transactions done electronically [4].

The current EMRs all have some privacy safeguards in place, and major healthcare institutions have taken steps to protect employees from looking up information on patients who the provider does not manage or treat directly. Despite these protections, numerous potential intrusions into patient privacy are possible with the current commercial systems [3]. Centralization of medical records in the increasing number of multi-group and systems practices distributes personal medical data over larger networks and increases the likelihood that personal medical data may be shared or viewed by unauthorized users. While large systems may have active monitoring of unauthorized access to medical records, smaller satellite offices may not have the same ability to monitor who is accessing patient records [5].

This article will review the benefits of EMRs and the issues of patient confidentiality the electronic medical record presents. In addition, the possible mechanisms by which data may be shared without patient knowledge as well as solutions and safeguards that may need to be taken to protect the privacy of patient medical records will be reported in this article.

BENEFITS OF ELECTRONIC MEDICAL RECORDS

For thirty years the idea of placing patients' medical records

on the computer has been discussed, but it is only in the last decade that it has become widely adopted [6].The Institute of Medicine has put forth eight core functions for the electronic medical record including; health information and data; result management; order management; decision support; electronic communication and connectivity; patient support; administrative processes and reporting; reporting and population health.

Benefits of electronic medical records are also purported to include decreased medication errors, links to health insurance benefits so providers know which medications are covered, and associated with quality care standards [7]. Other advantages include improved use of radiology tests, enhanced capture of charges, and a reduction in billing errors, which allows the government to access comparable national health data for planning and research [4]. Another positive aspect of the electronic medical record is the possibility of ensuring large numbers of cases with identifying information will be stripped of identifiers for purposes of medical research on large aggregates with particular disease conditions or exposures. EMRs have provided new opportunities for clinical research including the execution of clinical trials for new medications [8]. Having the ability to link recently published care standards with targeted patient groups who may be eligible for clinical trials may improve access to the latest treatments for patients. However, some experts in the health communication field have argued that the electronic health record has improved the administrative functioning of healthcare, but not necessarily the clinical care experience for the patient [9].

LEGAL AND ETHICAL CONCERNS OF CLINICAL RESEARCH

The possibilities of using large patient databases for clinical trials and other clinical research studies are numerous and could lead to more efficient data gathering and clinical advances for the population. However, there are some technical difficulties with systems working together utilizing large databases and this may make it difficult to obtain individual consent for studies and laws concerning research on electronic data sets vary by country and jurisdiction [7]. In some countries explicit consent is not needed for using coded EMR data if these data are considered to provide research information in the interest of public health. Another approach involves making the data anonymous so individual patients cannot be recognized before its use. These communication concerns are issues institutions are still resolving with their EMR systems and research studies.

ISSUES OF PATIENT CONFIDENTIALITY

EMRs are thought to increase efficiency and provide cost savings; however they increase the risk to privacy of patient medical records [4]. There have been numerous individual complaints on the Health Insurance Portability and Accountability Act (HIPAA) violations as well as a rather well-known case of an Administrative Assistant at the University of California at Los Angeles (UCLA) indicted for disclosing medical records of celebrity patients [4]. Transferring records from one practice to the other may also present problems for patient privacy.

The United States government stance on privacy issues since the events of 9/11 has become less stringent allowing many governmental entities to view personal records of citizens. Private medical records are available to law enforcement officials without a warrant under many circumstances [4]. Once medical data are stored in a centralized environment there are few limits to who can request access via court order. In addition to unauthorized access, there is legal access which may be gained from law enforcement with a warrant. Under the Patriot Act, the FBI may obtain records to protect against terrorism or for clandestine intelligence activities.

The Affordable Care Act has led to a reduction in health insurers not providing insurance for those persons with pre-existing conditions, so the fear of not receiving health insurance is no longer a potential worry. However, the medical diagnoses and treatment plans that are submitted to insurance companies may still be accessed by data mining organizations and the ability to view these data may potentially affect a patient's ability to obtain life insurance or potentially employment [5]. There is also the issue of the curious healthcare workers and student interns in healthcare settings accessing neighbors and friends electronic medical records without authorization.

Privacy can also be violated through employers, health or life insurance coverage or participation in government benefit programs. If an employee is investigated for occupational and safety violations the health records of the employee may become part of the case file. This may be the exchange for some type of compensation for the employee. The Medical Information Bureau, Intelliscript, and Med Point all collect health information on consumers much like credit bureaus [4]. This information is shared with insurance companies to evaluate applicants. Medical records and health history may also be disclosed during quality reviews of providers as well as through the search of an individual's computer who may have been searching health information online. Increasing health care costs have encouraged self management of one's health. Health information technology allows patients to manage their own health care online [10]. However, these searches may leave them vulnerable to tracking of search terms concerning medical issues in building marketing profiles of individual computer users.

The dissemination of such large volumes of data in electronic format has increased the risk for exposure of confidentiality of patient data. In the 2009, the Ponemon report titled "Electronic Health Information- a Study of IT Practitioners", it was noted 80% of the healthcare organizations surveyed had at least one occurrence of a lost or stolen medical record. [11]. This study surveyed over 500 Information Technology (IT) professionals in healthcare organizations in the United States who had implemented the electronic health record. The general feeling of the IT professionals were that their own organizations did not have enough safeguards in place and that the majority of senior management (70 %;n=350) interviewed did not see patient privacy as a priority [11].

RISKS AND CONSEQUENCES OF SOCIAL MEDIA

In addition to the risk of sharing private patient information through official electronic records, the frequency of cell phones and personal computers or tablets in the workplace can present problems with healthcare workers sharing private information

on social media sites. One of the disadvantages of social media sites is that once a post is made, a permanent digital footprint is created. Simply liking a page or friending a patient can lead to situations which violate patient confidentiality and may leave healthcare workers in precarious legal situations.

Other situations relating to sharing confidential patient data may involve a lack of knowledge or forethought on the part of healthcare workers. Social media removes rules and boundaries which the normal workplace procedures protect against, in all instances. Officially, healthcare workers may not share personal private patient information outside the "covered entity" without the patients consent; however there have been some fairly egregious violations of this rule. In one case, a group of nurses used Facebook to provide shift change reports containing specific information on patients. Information was passed on to their 'friends" violating federal privacy regulations (Ayers, 2013). In another case, healthcare workers posted pictures of a patient record on a social media site, an obvious violation of HIPAA. Healthcare professionals must monitor their presence to make sure information is accurate and professional

SAFETY ISSUES

Although part of the argument for the use of the electronic medical records has been to increase medication safety, there have been reported safety issues with medications depending on computer documentation to obtain the right medication, right dose, and right patient. The data which are viewed are only as good as the data entered; there is still the possibility of human error in entering data. Different programs or applications might not link the right medication to the order [8]. The Agency for Healthcare Research and Quality (AHRQ) estimates once fully installed electronic medical health systems may cause 60,000 adverse events per year (Freudenheim, 2012).

Another issue of concern is that although EHRs help make billing more efficient, these records may lead to more fraudulent billing [8]. Using checklists that require pointing and clicking may lead busy practitioners to check off more assessments than they have actually performed and resulting in higher billing.

SOLUTIONS/SAFEGUARDS TO PROTECT PRIVATE PATIENT INFORMATION

The new Health Information Technology for Economic and Clinical Health Act (HITECH) which offers federal assistance to encourage adoption of EHR also has strict rules for data security. These regulations require increased audits and mandatory patient data breach notification requirements. In addition to the provisions of the HITECH act, there is a federal ban on the sale of medical records except for the exchange to "a business associate for activities that the business associate undertakes on behalf of and at the request of the company holding the private information". Consumer watchdog groups do not feel this provides enough protection and suggests even greater privacy protections.

The American Civil Liberties Union (ACLU) has been critical of the strong promotion for medical practices to accept the EMR because of potential problems of identity theft, accidental publication of personal information; discrimination by employers or life insurance companies, and the potential commercial resale of information and invasive direct marketing of consumers [4]. Proposed solutions include expanding the scope of the national privacy legislation to encompass the entire medical marketplace and enabling patients' control of their data with a choice to opt out of sharing information without their permission. In addition, prompt patient notification of data breaches and mandatory use of data security safeguards are resolutions to this concern.

Consumer watchdog group suggest the following steps to ensure confidentiality of private patient information:

1. Providing an audit trail to track who accesses the EMRs;
2. Holding database managers and organizations accountable for keeping the EMRs private including removing any safe harbor provisions in legislation that would protect organizations from being accountable for unintentional disclosures;
3. Allowing states to adopt more protective standards to establish additional privacy regulations;
4. Making health data unusable or unreadable by unauthorized users;

PATIENT EDUCATION AND PROTECTION OF CONFIDENTIAL INFORMATION

EMRs may also be disclosed during quality reviews of providers, or for health research. Practices have been urged to give patients access to their electronic medical record as well, although this practice is not yet widespread [12]. Healthcare providers need to be vigilant in keeping patient's medical information private and aware of all the HIPAA regulations which established protection for all personally identifiable information stored in electronic format [6]. Providers need to better explain to their patients what information is being passed on to other health care providers. Patients should be given the option of not having their data from a specific visit or specialty shared within broader health care networks. Having all the specialty records connected in one EMR may afford easier access to the provider in need of data, however a patient may not want to share a private conversation in a specialist's office on a sensitive topic. The dissemination of such large volumes of data in electronic format has increased the risk for breaks in confidentiality of patient data [4]. Progressive institutions, such as the Mayo Clinic, allow patients instant access of records via their I-phones [8].

A major question to be answered for consumers is how medical data will be shared with insurance companies and other corporations and government agencies. The Medical Information Bureau, Intelliscript and Med Point all collect health information on consumers much like credit bureaus and this information is shared with insurance companies to evaluate applicants [4]. Some states are considering allowing patients to limit who will view their medical records . http://phys.org/news/2010-11-electronic-medical-pprivacy.html

Decentralized storage systems are one solution. The state of Maryland is starting a central patient registry that would link all doctors, hospitals, and laboratories and has worked out strict privacy rules. Records shared among many agencies

increase the risk of unauthorized exposure of patient's records and the risk of the computer systems that store them being hacked. Experts note that these systems are not ready yet and testing is occurring on patients without their consent. There has been a call for more research by the Institute of Medicine on patient safety issues with EMRs and an end to the hold harmless clause that protects software manufacturers from lawsuits [8]. Patient rights' advocates also call for hospitals to reject clauses in contracts from software vendors to not hold them liable and require that software manufacturers report deaths and serious injuries caused by IT programs.

CONCLUSIONS

EMRs have brought about a host of benefits for clinical research, billing, patient record keeping and access of clinicians to patients medical history, laboratories, and radiology tests. However, the privacy issues associated with the EMR need to be better understood and individual patient confidentiality needs to be protected. As the EMR becomes more standard in healthcare systems, continued vigilance is needed to protect patient privacy by healthcare providers, legislators, healthcare administrators, and information technology specialists. Patients should have uncomplicated access to their medical records and the right to limit information shared with other entities.

REFERENCES

1. Holve E, Calonge N. Lessons from the Electronic Data Methods Forum: collaboration at the frontier of comparative effectiveness research, patient-centered outcomes research, and quality improvement. Med Care. 2013 Aug; 51:S1-S3.
2. Health Information Technology Policy Committee. Meaningful use workgroup request for comments regarding meaningful use stage. http://www.healthit.gov/policy-researchers-implementers/meaningful-use-stage-2. Accessed December 1, 2013.
3. Kraschnewski JL, Gabbay RA . Role of health information technologies in the Patient-centered Medical Home. J Diabetes Sci Technol. 2013; 7: 1376-1385.
4. Walker JM, Carayon P, Leveson N, Paulus RA, Tooker J, Chin H, Bothe A Jr . EHR safety: the way forward to safe and effective systems. See comment in PubMed Commons below J Am Med Inform Assoc. 2008; 15: 272-277.
5. Harrison PJ, Ramanujan S. Electronic medical records: Great idea or Great Threat to privacy Review of Business information Systems. 2011; 15: 1
6. Singh H, Ash JS, Sittig DF. Safety assurance factors for electronic health record resilience (SAFER): study protocol. Medical Informatics & Decision Making. 2013.
7. Gartee, R & Beal, S. Electronic Health Records and Nursing. 2012;Pearsons, Boston.
8. Coorevits P, Sundgren M, Klein GO, Bahr A, Claerhout B, Daniel C, et al . Electronic health records: new opportunities for clinical research. J Intern Med. 2013; 274: 547-560.
9. Freudenheim, Milt, "The Ups and Downs of Electronic Medical records" New York Times. 2012.
10. Zarcadoolas C, Vaughon WL, Czaja SJ, Levy J, Rockoff ML . Consumers' perceptions of patient-accessible electronic medical records. J Med Internet Res. 2013; 15: 168.
11. Ayres EJ. The impact of social media on business and ethical practices in dietetics. J Acad Nutr Diet. 2013; 113: 1539-1543.
12. Vodicka E, Mejilla R, Leveille SG, Ralston JD, Darer JD, Delbanco T, et al. Online access to doctors' notes: patient concerns about privacy. J Med Internet Research. 2013; 15: 208.

Cite this article

Aselton PJ, Affenito S (2014) Privacy Issues with the Electronic Medical Record. Ann Nurs Pract 1(2): 1009.