Review Article

Ethical issues in electronic health records: A general overview

Fouzia F. Ozair,
Nayer Jamshed[1],
Amit Sharma[2],
Praveen Aggarwal[1]

Department of Health Services,
Jawahar Lal Nehru University,
[1]Department of Emergency Medicine,
All India Institute of Medical Sciences,
[2]Department of Forensic Medicine,
Hamdard Institute of Medical Sciences
and Research, New Delhi, India

Address for correspondence:
Dr. Nayer Jamshed,
Department of Emergency Medicine,
All India Institute of Medical
Sciences, Aurobindo Marg,
New Delhi - 110 029, India.
E-mail: jamshednayer@gmail.com

Abstract

Electronic health record (EHR) is increasingly being implemented in many developing countries. It is the need of the hour because it improves the quality of health care and is also cost-effective. Technologies can introduce some hazards hence safety of information in the system is a real challenge. Recent news of security breaches has put a question mark on this system. Despite its increased usefulness, and increasing enthusiasm in its adoption, not much attention is being paid to the ethical issues that might arise. Securing EHR with an encrypted password is a probable option. The purpose of this article is to discuss the various ethical issues arising in the use of the EHRs and their possible solutions.

Key words: Confidentiality, electronic health record, paper record, security breaches

INTRODUCTION

An electronic health record (EHR) is a record of a patient's medical details (including history, physical examination, investigations and treatment) in digital format. Physicians and hospitals are implementing EHRs because they offer several advantages over paper records. They increase access to health care, improve the quality of care and decrease costs. However, ethical issues related to EHRs confront health personnel. When patient's health data are shared or linked without the patients' knowledge, autonomy is jeopardized. The patient may conceal information due to lack of confidence in the security of the system having their data. As a consequence, their treatment may be compromised. There is the risk of revelation of thousands of patients' health data through mistakes or theft. Leaders, health personnel and policy makers should discuss the ethical implications of EHRs and formulate policies in this regard. The electronic medical record (EMR) is the tool that promises to provide the platform from which new functionality and new services can be provided for patients.

Access this article online

Quick Response Code:

Website:
www.picronline.org

DOI:
10.4103/2229-3485.153997

POTENTIAL BENEFITS

A medical record in the past was information documented on paper for research, clinical, administrative and financial purposes. Its major drawback was in terms of accessibility, and it was available to one user at a time. Its completion was delayed anywhere from 1 to 6 months or more because it was updated manually.[1]

The purpose of documentation through electronic media remains the same even today that is to support patient care. EHRs have several advantages over paper records. Production of legible records reduces many problems of wrong prescriptions, doses and procedure.[2] Moreover adverse drug reactions can be reduced substantially when the EHRs are connected to drug banks and pharmacies. This can be done by not permitting prescription and order for drugs for which a known adverse reaction is known for a certain patient.[2] Easy accessibility from anywhere at any given time is also beneficial.[3] They require less storage space and can be stored indefinitely. They reduce the number of lost records, help research activities, allow for a complete set of backup records at low cost, speed data transfer and are cost-effective.[4,5] Hence, EHRs have been shown to improve patient compliance, facilitate quality assurance and reduce medical errors.[6]

The office of the National Coordinator for Health Information Technology (IT) refers to the health record as "not just a collection of data that you are guarding, it is life."[7] The patient owns the information in the record. The physician and the organization is the owner of the physical medical record.[8] There are four major ethical priorities for EHRS: Privacy and confidentiality, security breaches, system implementation, and data inaccuracies.

PRIVACY AND CONFIDENTIALITY

Justice Samuel Dennis Warren and Justice Louis Brandeis define privacy as the right "to be let alone."[9] The other definition given by Richard Rognehaugh is as the right of an individual to keep information about themselves from being disclosed to others; the claim of individuals to be let alone, from surveillance or interference from other individuals, organizations or the government.[10] Information of a patient should be released to others only with the patient's permission or allowed by law. When a patient is unable to do so because of age, mental incapacity the decisions about information sharing should be made by the legal representative or legal guardian of the patient. Information shared as a result of clinical interaction is considered confidential and must be protected.[11] Information from which the identity of the patient cannot be ascertained for example, the number of patients with breast carcinoma in a government hospital, is not in this category.[12]

Health care institutions, insurance companies and others will require access to the data if EHRs are to function as designed. The key to preserving confidentiality is to allow only authorized individuals to have access to information. This begins with authorizing users. The user's access is based on preestablished role-based privileges. The administrator identifies the user, determines the level of information to be shared and assigns usernames and passwords. The user should be aware that they will be accountable for the use and misuse of the information they view. They have access to the information they need to carry out their responsibilities. Hence assigning user privileges is a major aspect of medical record security.[13]

Although controlling access to health information is important, but is not sufficient for protecting the confidentiality. Additional security steps such as strong privacy and security policies are essential to secure patient's information.

SECURITY BREACHES

Security breaches threaten patient privacy when confidential health information is made available to others without the individual's consent or authorization. Two recent incidents at Howard University Hospital, Washington showed that inadequate data security can affect a large number of people. On May 14, 2013, federal prosecutors charged one of the hospital's medical technicians with violating the Health Insurance Portability and Accountability Act (HIPAA). Prosecutors said that over a 17-month period, Laurie Napper used her position at the hospital to gain access to patients' names, addresses and Medicare numbers in order to sell their information. A plea hearing had been set for June 12, 2013 in which she was found guilty and sentenced for 6 months in a half-way house and fined $2,100. A few weeks earlier, the same hospital informed more than 34,000 patients that their medical data had been compromised. A contractor working with the hospital had downloaded the patient's files onto a personal laptop, which was stolen from his car. The data were password protected, but unencrypted, which means anyone who guessed the password could have accessed the patient files without a randomly generated key. By encryption, we mean encoding of information in such a way that only authorized parties can read it. It is usually done with the help of encryption key, which specifies that how the information should be decoded. According to a hospital press release, those files included names, addresses, and Social Security numbers and in a few cases, "diagnosis related information". Recently a hospital chain named Prime Health care Services Inc. has agreed to pay $275,000 to settle a federal investigation into alleged violation of patient privacy. Keeping records secure is a challenge that doctors, public health officials and federal regulators are just beginning to understand. Cloud storage, password protection, and encryption are all measures health care providers can take to make portable EHRs more secure. A survey conducted found that 73% of physicians text other physicians about work.[14] Mobile devices are for individual use and are not designed for centralized management by an IT Department.[15] Mobile devices can easily be misplaced, damaged, or stolen. Emphasis must be laid on encrypting mobile devices that are used to transmit confidential information. Portable EHRs can be made more secure by using cloud storage, password protection, and encryption. Usage of two factor authentication system with security tokens and password are helpful in securing EHRs.

Security measures such as firewalls, antivirus software, and intrusion detection software must be included to protect data integrity. Specific policies and procedures serve to maintain patient privacy and confidentiality. For example, employees must not share their ID with anyone, always log off when leaving a terminal and use their own ID to access patient digital records. A security officer must be designated by the organization to work with a team of health IT experts.

Routine random audits should be conducted on a regular basis to ensure compliance with hospital policy. All system activity can be tracked by audit trails. This includes detailed listings of content, duration and the user; generating date and time for entries and logs of all modifications to EHRs.[16] When there is inappropriate access to a medical record, the system can yield information about the name of the individual gaining access; the time, date, screens accessed and the duration of the review. This information is useful when determining whether the access is the result of an error or an intentional, unauthorized view. The HIPAA Security Rule requires organizations to conduct audit trails, requiring that they document information systems activity[17] and have the hardware, software, and procedures to record and examine activity in systems that contain health information.[18]

Outside vendors create special privacy issues. Employee-only access to the EMR requires any external vendor to access and navigate the record under the authorization and oversight of an employee.

SYSTEM IMPLEMENTATION

Health care organizations encounter major challenges in the course of EHR implementation these challenges result in wasted resources, frustrated providers, loss of confidence by patients and patient safety issues. The development, implementation, and maintenance of EHRs requires adequate funds and the involvement of many individuals, including clinicians, information technologists, educators, and consultants.[19]

Hospitals and health care institutions are making improvements without significant clinician engagements. Many EHR implementation projects fail because they underestimate the importance of one or more clinician to serve as opinion leaders for providers in the clinic. Thus, clinician must guide colleagues in understanding their roles in the implementation and enlisting their involvement in tasks as EHR selection, workflow design, and quality improvement.[20]

Clinical personnel often have little knowledge of the clinic's workflow and the roles others play in care delivery. This blind spot results in inadequate planning for successful implementation. Without identifying a standardized best practice method to do the work, every user is left to struggle. Clinics should map and standardize their workflows before EHR selection.

When any two systems are integrated, an interface is created. By the user interface, we mean an interface between the user and the computer system. These interfaces are critical to the overall success of the implementation process. Interface issues are the greatest system risk because these failures can be invisible initially. Lack of systemic consideration of users and tasks often results in poor user interface. Poorly designed user interface account for unintended adverse consequence leading to decreased time efficiency, poor quality of care and increased threat to patient safety. Improperly designed user interface fail to deliver the much needed quality of care, which lead to user dissatisfaction. The faulty user interface issue, which was small earlier on, increases over a period of time that leads to abandonment of EHR. Maintenance and testing of these interfaces on a routine basis is essential in controlling this major risk. Practice disruption during EHR implementation can negatively impact the quality of care or endanger patient safety along with financial loss.[21]

DATA INACCURACIES

Integrity assures that the data is accurate and has not been changed. EHRs serve as a way to improve the patient's safety by reducing healthcare errors, reduce health disparities and improve the health of the public.[22] However, concerns have been raised about the accuracy and reliability of data entered into the electronic record.

Inaccurate representation of the patient's current condition and treatment occurs due to improper use of options such as "cut and paste". This practice is unacceptable because it increases the risk for patients and liability for clinicians and organizations.[16,23] Another feature that can cause a problem in the data integrity is the drop down menu and disposition of relevant information in the trash. Such menus limit the choices available to the clinician who in a hurry may choose the wrong one leading to major errors. Clinicians and vendors have been working to resolve software problems to make EHRs both user-friendly and accurate.[23]

Loss or destruction of data occurs during data transfer; this raises concerns about the accuracy of the data base as patient care decisions are based on them.[24] A growing problem is of medical identity theft. This results in the input of inaccurate information into the record of the victim. The person's insurance company is billed for medical services not provided to the actual policy holder and the patient's future treatment is guided by misinformation that neither the patient nor provider immediately recognize.

ELECTRONIC HEALTH RECORDS IN INDIA

India is providing quality health care of international standards at a relatively low cost and has attracted the patients from across the globe. India is now one of the favorite destinations for the health care services. Considering rapid pace of growth of health care sector in India, Government of India in April 2013, came out with definitive guidelines for EHR standards in India. Guidelines were based on the recommendations made by EMR standards committee, which was constituted by an order of Ministry of Health and Family Welfare. It was coordinated by Federation of Indian Chambers of Commerce and Industry on its behalf. The guidelines recommend set of standards to be followed by different health care service providers in India and hence that medical data becomes portable and easily transferable.[25] India having a population of 1.27 billion people with only 160 million internet users maintenance of EHR is a daunting task, but with the interest and support of the Government of India in its implementation, it will a success soon.

CONCLUSION

Regardless of one's role, everyone will need the assistance of the computer. Creating a useful EHR system will require the expertise of physicians, technology professionals, ethicists, administrative personnel, and patients. Although EMRs offer many significant benefits, the future of health care demands that their risks be recognized and properly managed or overcome. Multiple strategies are available to reduce risks and overcome barriers in the implementation of digital health records. Leadership, teamwork, flexibility, and adaptability are keys to finding solutions. EMRs capacities must be maximized in order to enhance improve the quality, safety, efficiency, and effectiveness of health care and health care delivery systems.

REFERENCES

1. Poissant L, Pereira J, Tamblyn R, Kawasumi Y. The impact of electronic health records on time efficiency of physicians and nurses: A systematic review. J Am Med Inform Assoc 2005;12:505-16.
2. Sanbar SS. Medical records: Paper and electronic. In: American College of Legal Medicine Textbook Committee. Legal Medicine. 6th ed. St. Louis: Mosby; 2004.
3. Anderson JG. Social, ethical and legal barriers to e-health. Int J Med Inform 2007;76:480-3.
4. Stanberry B. Telemedicine: Barriers and opportunities in the 21st century. J Intern Med 2000;247:615-28.
5. Stone AA, Shiffman S, Schwartz JE, Broderick JE, Hufford MR. Patient compliance with paper and electronic diaries. Control Clin Trials 2003;24:182-99.
6. Lo B. Professionalism in the age of computerised medical records. Singapore Med J 2006;47:1018-22.
7. Office of the National Coordinator for Health Information Technology. Guide to privacy and security of health information. 2012. p. 5. Available from: http://www.healthhit.gov [Last accessed 2014 Jan 05].
8. Odom-Wesley B, Brown D, Meyers CL. Documentation of Medical Records. Chicago: American Health Information Management Association; 2009. p. 21.
9. Warren SD, Brandeis LD. The right to privacy. Harv Law Rev 1890;4:193.
10. Rognehaugh R. The Health Information Technology Dictionary. Gaithersburg, MD: Aspen; 1999. p. 125.
11. Rinehart-Thompson LA, Harman LB. Privacy and confidentiality. In: Harman LB, editor. Ethical Challenges in the Management of Health Information. 2nd ed. Sudbury, MA: Jones and Bartlett; 2006. p. 53.
12. Rinehart-Thompson LA, Harman LB. Privacy and confidentiality. Ethical Challenges in the Management of Health Information. 2nd ed. Sudbury, MA: Jones and Bartlett; 2006. Chapter 3, p. 54.
13. American Health Information Management Association. The 10 security domains (updated). J Am Health Inf Management Assoc 2012;83:50.
14. Greene AH. HHS steps up HIPAA audits. J AHIMA 2011;82:58-9.
15. Hughes G. Mobile device security (updated). J AHIMA 2012;83:50-5.
16. American Health Information Management Association. Copy functionality toolkit. 2008. p. 4. Available from: http://library.ahima.org [Last accessed on 2014 Jan 05].
17. US Department of Health and Human Services. Security standards: General rules, 46 CFR section 164.308(a)-(c).
18. US Department of Health and Human Services. Technical safeguards. 45 CFR section 164.312 (b).
19. Bostrom AC, Schafer P, Dontje K, Pohl JM, Nagelkerk J, Cavanagh SJ. Electronic health record: Implementation across the Michigan Academic Consortium. Comput Inform Nurs 2006;24:44-52.
20. Reinertsen JL, Gosfield AG, Rupp W, Whittington JW. Engaging Physicians in a Shared Quality Agenda. IHI Innovation Series white paper. Cambridge, Massachusetts: Institute for Healthcare Improvement; 2007. Available from: www.IHI.org [Last accessed on 2014 Jan 05].
21. Menachemi N, Ford EW, Beitsch LM, Brooks RG. Incomplete EHR adoption: Late uptake of patient safety and cost control functions. Am J Med Qual 2007;22:319-26.
22. American Recovery and Reinvestment Act, HR 1, 111th Congress, 1st Session; 2009.
23. Gelzer R, Hall T, Liette E, Reeves MG, Sundby J, Tegen A, *et al*. Auditing copy and paste. J AHIMA 2009;80:26-9.
24. North Carolina Healthcare Information and Communications Alliance, Inc. The benefits and risks of electronic health records.
25. E.H.R. Standards for India: GOI Report; April 2013. Available from: http://www.mohfw.nic [Last accessed on 2014 Apr 15].

How to cite this article: Ozair FF, Jamshed N, Sharma A, Aggarwal P. Ethical issues in electronic health records: A general overview. Perspect Clin Res 2015;6:73-6.

Source of Support: Nil. **Conflict of Interest:** None declared.