Electronic Medical Records: Great Idea Or Great Threat To Privacy?

P.J. Harrison, University of Central Missouri, USA
Sam Ramanujan, University of Central Missouri, USA

ABSTRACT

The practice of storing health care records in electronic format, rather than the traditional paper, is becoming increasing popular, especially since the advent of legislation that provided a framework for transmission of these data and encouragement to convert. However, this process is not without challenges and there are significant concerns over how to maintain the security of these data. On one hand, EMRs are expected to increase efficiency and provide cost savings. On the other hand, they increase the risk to privacy. This paper discusses both the risks and benefits of EMRs in the current legal framework in order for us to gain a better understanding of these systems. Awareness of the risks will help in building more secure EMRs which may be mandated in most countries.

Keywords: Electronic Medical Records (EMR); Healthcare Informatics; Information Systems; Legal issues in IT, Privacy

INTRODUCTION

The practice of storing health care records in electronic format, rather than the traditional paper, is becoming increasing popular, especially since the advent of legislation that provided a framework for transmission of these data and encouragement to convert. However, this process is not without challenges and there are significant concerns over how to maintain the security of these data. Proponents of electronic data tout the benefits gained, including increased efficiency and cost savings. Opponents argue the benefits are not worth the risk to privacy. Therefore, are health records stored in electronic format the greatest idea since the invention of the mouse trap, or is this one more way in which our personal rights to privacy are being eroded? In order to address this issue, this paper first discusses the history of Electronic Medical Records (EMR). This is followed by an analysis of the current issues in EMR. In particular, we focus on the costs/benefits of EMR and threats to privacy posed by such recording of medical data. Next, we provide a discussion of the future of EMR based on current trends in technology and demographic changes. Finally, the conclusions of the study are presented.

HISTORY OF ELECTRONIC MEDICAL RECORDS

The Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) or “HIPAA” established, for the first time, a set of regulations to standardize the collection, storage, and dissemination of individually identifiable health information. The confidentiality of health records is covered in two key rules: the Electronic Data Interchange Rule and the Privacy Rule. The rule requiring adoption of a national standard for electronic health care transactions by the Department of Health and Human Services is known as the Electronic Data Interchange rule. This rule requires the consistent use of health care transactions, code sets, and identifiers for every provider who does business electronically. It is commonly thought the impetus behind this legislation was the desire for all Medicare transactions to occur electronically; before this could occur, the privacy and security of electronic medical records (EMRs) needed to be addressed.

As Congress recognized the privacy of health information could be eroded by advancing technology, provisions were incorporated into this legislation that mandated the adoption of federal privacy protections for individually identifiable health information. In response to this mandate, the Privacy Rule was published in

December 2000, to become effective on April 14, 2001. Following a period of public review and comments, the final modified Privacy Rule was adopted in August 2002. This Privacy rule was intended to allow the flow of health information for high-quality health care while protecting the privacy of individual health information. According to the Department of Health and Human Services, Office of Civil Rights, the information protected under the Privacy Rule is defined as:

"…all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."

"Individually identifiable health information" is any information that can either identify an individual or provide a reasonable belief it could be used to identify an individual. Such information may include, but is not limited to, demographic data (gender or race), name, address, date of birth, or Social Security number as well as past, present, or future physical/mental health information. However, the use of de-identified health information has no restrictions. Entities covered under the HIPAA regulations include insurance companies, health care providers, and healthcare clearinghouses who transmit health care data in electronic format. All covered entities, including small health plans, were expected to be in compliance with HIPAA by April 14, 2004 or face civil penalties for noncompliance.

Since the advent of HIPAA, there have been numerous legislative attempts to encourage the adaptation of health information technology (IT) systems. However, most of these attempts have failed, in large part, due to weak protections of patient privacy. There are two important bills currently in progress that may encourage the switch to EMRs nationwide.

1. In September 2008, Rep. Pete Stark introduced HR 6898[1] that would use the Medicare payment system to reward physicians who implement health IT systems while late adopters or those who fail to switch could be penalized. This bill also proposes the creation of a federal advisory committee charged with the responsibility of creating a set of standards for interoperability, security, and the clinical use of health IT.
2. The Protecting Records, Optimizing Treatment and Easing Communications Through Healthcare Technology Act, or PRO(TECH)T Act[2], which is still pending consideration by the House of Representatives, funds grants and loans for the implementation of health IT systems and also provides stronger patient privacy and security. However, opponents have expressed concerns that the bill may leave patients vulnerable to misused or lost data as the privacy protection afforded is not strong enough.

Whether or not these bills will be approved remains to be seen. However, given the large number of proposed legislation attempted and discarded, it is apparent US lawmakers are anxious to further refine the concepts first established by HIPAA.

CURRENT ISSUES

In this section we will delve into the consequences of adopting EMR in the purview of the current legal framework. This is accomplished by first evaluating the benefits and risks in adopting EMR. This is followed by the analysis of the impact of EMR on privacy.

Benefits and Risks

Proponents of HIPAA argue the regulations would help reduce waste and fraud in the health care system as well as provide a national framework for privacy, security, and standardized transmissions of electronic health care transactions. Specifically, standardized transactions are expected to:

[1] Current Status: Referred to the Subcommittee on Technology and Innovation.

[2] Current Status: Cleared by the House Energy and Commerce committee.

- make data processing more efficient;
- allow for more comparable national health care data, which will lead to improved health care delivery and increased public knowledge as a result of better analysis and research; and
- lead to improved software, which will, in turn, create more efficiency in processing transactions.

Furthermore, proponents say that converting to electronic health records via new health IT software and hardware will reduce medical errors, improve patient care, and save money. Additional benefits of EMRs include the ease of keeping patient records up to date and easily accessible when needed, ease of tracking of patients for follow-up care, ease of incorporating all patient information in one location, and ability to analyze large amounts of data for long term trends.

The challenges associated with the use of EMRs include the training of data entry personnel; the cost associated with establishing IT systems; the need to have long-term resources for development and support; concerns over security of patient data; and the need to ensure a stable power supply and proper data backup.

A Wall Street Journal Online/Harris Interactive poll from 2007 indicated most Americans believe EMRs have the potential to improve healthcare in the United States and that benefits outweigh risks. A total of 74% of the respondents indicated patients could receive better care if providers had easier access to medical records via EMRs and 62% responded the use of EMRs can decrease the number of medical errors. There were 60% of respondents who agreed the benefits of EMRs outweigh the risk to privacy. Conversely, a Harris Interactive poll conducted in 2004 indicated the biggest concerns people have about keeping online medical records are threats to privacy 68% and security 66%.

A study conducted by Dr. Samuel J. Wang, et al, at the Department of Information Systems, Partners HealthCare System (Boston, Massachusetts) to estimate the net financial benefit or cost of implementing electronic medical record systems in primary care found the estimated benefit was $86,400 per provider for the 5-year period studied. The study found the primary savings were in drug expenditures, improved use of radiology tests, improved capture of charges, and a decrease in billing errors, which led to their conclusion that the implementation of EMR system can result in positive financial return to a health care organization.

A panel proposal entitled “What is Wrong with EMR?”, which was submitted for consideration at AMIA99 (The 1999 Annual Symposium of the American Medical Informatics Association) postulated the following ideals for EMRs:

“EMR has the potential to make a highly significant contribution to the advancement of medicine and to the improvement of the quality of healthcare. An ideal EMR should be able to provide complete, accurate, and timely data, alerts, reminders, clinical decision supports, medical knowledge, communications, and other aids at all points of care for all healthcare professionals at all times in a way the quality of healthcare can be dramatically improved. It should include the old useful functions and overcome the known problems of paper-based records, provide new useful functions that are not available from paper-based records, and at the same time it should not generate new problems associated with the electronic medium.”

The need for greater efficiency has driven the integration of health IT systems into hospitals and large medical practices. It is hoped the new systems will provide increased efficiencies and better patient care while trying to maintain a tight budget. Although protection of patient privacy is of utmost concerns in the implementation of health IT systems, it seems that most consumers are willing to take some risks to enjoy the benefits of EMRs.

Threats to Privacy

By all accounts, it seems the biggest hurdle to large-scale implementation of EMRs is the need to properly secure patient data from those who would snoop into the health information of others. The assurance of greater security will lead to greater adoption of electronic transactions, which will also enable the healthcare industry to improve the level of service. Because HIPAA is a law that was intended to protect consumers from exploitation of their personal health information by insurance companies, employers, or those with malicious intent, healthcare providers can build the loyalty of patients and reduce the risk of litigation by complying with the due diligence requirements of HIPAA. Properly secured records are at a lower risk of unauthorized access or being stolen. The Department of Justice can impose stiff penalties of up to $100 per violation for noncompliance with HIPAA. While this seems a small amount, the fines are quickly compounded for unauthorized access to even a small database containing patient records.

Despite the requirements of HIPAA and potential of large fines for noncompliance, and despite the good intentions of healthcare providers, it seems there have been an inordinate number of complaints related to privacy violations. A few of the most recent cases include the following:

- A patient of the National Health Service (NHS) in the United Kingdom filed a complaint that her "private and confidential" records were included in a database, which was accessible to staff at her local health counsel. Her claim is that inclusion of her records in the database occurred without her permission.
- A former administrative specialist at the University of California – Los Angeles (UCLA) was indicted by a federal grand jury for HIPAA violations. She was accused of disclosing health records of celebrity patients at the medical center in return for cash payments.
- According to an investigation by Pulse Magazine, there were 273 data security breaches from January 2007 until September 2007 at the NHS. Of these cases, 190 were related to breaches of privacy rules or unauthorized access and 83 were related to lost data. However, only 15 of these cases resulted in disciplinary action; none of which led to staff suspension or dismissal.
- The Des Moines Register conducted a review of state and federal records since 2003 and found that approximately 38,000 US residents have filed complaints for HIPAA privacy violations with the HHS Office of Civil Rights. Of these, 56% were resolved without investigation and only 437 complaints (less than 2%) were referred for prosecution.

Clearly, there is much work to be done to ensure the security of patient records. However, only one of the cases above is strictly related to electronic data. Security breaches from snooping, from incompetence, or from carelessness all occur when using paper records as well. The ability of computer systems to store large amounts of data magnifies the problems and makes even an unintentional mistake into a significant civil rights violation.

In addition to the unauthorized access to medical records, there are a number of legal mechanisms that erode the privacy of health records. For example, private medical records are accessible to law enforcement without a warrant under a wide variety of circumstances. Access may be requested if the person is a victim of or a suspect in a crime; for national security and intelligence activities; or for protective services for the president. The Patriot Act allows the Federal Bureau of Investigation (FBI) to obtain a court order for medical records during an investigation to protect against international terrorism or clandestine intelligence activities, with some limitations imposed by the First Amendment.

The confidentiality of health records may also be compromised through employers, health or life insurance coverage, or participation in government benefits programs. For example, if an employer is investigated for occupational health and safety violations, the health records of the employees may become part of the case file. In these cases, it is likely the consumer had traded some degree of confidentiality for the benefits offered, such as receiving aid from a government program.

There are also a number of risks to the confidentiality of health care records, which are unknown to most people. For example, the Medical Information Bureau, IntelliScript, and MedPoint are all companies that collect health information on consumers, much like the information collected by credit bureaus. The information is then provided to insurance companies to evaluate applications for various type of insurance. While these companies are not covered under the HIPAA regulations, they are now covered under the Fair Credit Reporting Act (FCRA), which gives consumers the right to review their personal data in these databases and provide corrections. Other disclosures of health records can occur when healthcare providers are evaluated for their quality of service or for renewed licensure. Health information may be disclosed for the purpose of health research, such as to the Centers for Disease Control. Lastly, those who participate in informal health screenings may have their data sold to direct marketer.

Although risks to privacy of data have nearly always been present, even with paper systems, the collection and dissemination of large volumes of data in electronic format has increased the risks dramatically.

WHERE ARE WE HEADED?

As the baby-boom generation ages, it is expected that the need for adequate and efficient health care will dramatically increase. It is estimated that in the next four decades, the number of people over 85 will more than triple. Many of the efficiencies gained though the use of health IT systems will be critical to address these needs. The industry that will be hardest hit by this aging population is the long-term care providers. This group has been slow to adopt health IT thus far, and healthcare policy planners are concerned about their ability to implement systems to handle the influx of patients.

The field of biometrics, which is the use of fingerprints, palm vein patterns, retinal images, etc., has become of great interest to health IT providers. This technology was once considered for use only by top-secret government installations, but is now becoming almost commonplace in the world of healthcare. Fujitsu Computer Products has entered into an agreement with BayCare Health Systems to begin the use of palm vein authentication devices during patient registration and also for identification. Fujitsu claims a low false acceptance rate of 0.00008 percent and, in the first month of operation, more than 99% of patients elected to enroll. As with any security measures, there needs to be a balance in the system that provides optimal security while allowing access to authorized users.

The implementation of large databases of patient information, especially databases stored on-line, is expected to increase as more healthcare providers adopt health IT systems. The Harris Corporation has developed a key technology that enables the secure, multi-agency exchange of health information. This system is expected to allow healthcare providers to share patient information "seamlessly and privately, improving the quality of care and reducing costs." For example, this system would allow easy sharing of an EMR between the Department of Defense, Veteran's Affairs, and the Social Security Administration for a wounded veteran who is applying for disability benefits.

Regardless of the wonderful new and innovative technologies developed for the sharing of patient information, the threats to patient privacy remain at the forefront of the debate. Lauren Weinstein of People for Internet Responsibility (PFIR) has expressed a concern that government and industry are seeking to destroy personal liberty though the implementation of EMRs, rather than to save money or improve healthcare:

"The most serious problem is that once medical data is in a centralized environment, there are essentially no limits to who can come along with a court order (or in the case of the government, as we know, secret orders or illegal demands that can't usually be resisted) for access to that data. Service providers typically have no choice but to comply."

Dana Blankenhorn of ZDNet Healthcare seems to agree with Mr. Weinstein and compares the accessibility of health records on the web to the application of privacy laws, thus far, to other types of data on the Internet:

"We have certainly seen this in the case or ordinary Internet data, where anonymity is breached at the drop of a lawsuit, and where the government really thinks it can catch terrorist needles in the enormous web cache haystack. If we're to place mandatory data online - and health records data are mandatory - then we expect better protections than found for our IMs, emails, and blog comments. Trouble is there is always an excuse (pedophiles, terrorists, market manipulation) that can breach such privacy, excuses the public supports, and those excuses would still exist even with stiffer privacy laws."

The American Civil Liberties Union (ACLU) is highly critical of proposed legislation aimed at forcing doctors and health care providers to convert from paper to EMRs stored in searchable, web-based databases. The main concern is the pending bills do not have sufficient privacy and security protections, which they feel is, in part, due to lobbying efforts to eliminate delays in establishment of these incentives. The ACLU lists the following potential undesirable consequences of such legislation:

- Identity theft;
- Accidental publication of patients' sensitive or embarrassing personal information;
- Discriminatory review by insurance companies or potential employers so they can avoid paying for people who might be expensive to insure or employ;
- Invasive direct marketing to patients or doctors by competing drug companies; and
- Commercial resale or misuse of personal health information.

In the opinion of the ACLU, legislation needs to expand the scope of national privacy practices to include the medical marketplace in its entirety, rather than just the providers covered under HIPAA. They also feel HIPAA is not enough protection and measures should be implemented to ensure security against snoopers and hackers as well as to ensure privacy of EMRs. The ACLU urges inclusion of the following patient controls in any legislation for EMRs:

- Real patient control of data including patient's rights to review his/her files, correct bad data, block access to personal information, and the choice to opt out of the system;
- Prompt patient notification of database breaches by codified and enforced deadlines;
- Fair compensation for damages in the event patient data is misused or stolen;
- Fair, nondiscriminatory medical treatment for patients who opt out of the data system; and
- Mandatory use of data security safeguards such as encryption and other technologies.

CONCLUSIONS

The future of health informatics holds a great deal of promise – from new technology to secure systems to new legislation to ensure the protection of privacy rights. However, there are still concerns that those who wish to exploit our personal health care data will still be able to do so. There has never been a shortage of those who wish to cause harm or embarrassment to others; this is not a phenomenon peculiar to the age of electronic data. Since it certainly appears electronic health care databases are here to stay, it is our responsibility to demand all reasonable measures are implemented to protect our data from intrusion or error. So, it seems EMRs are both a great idea and a great threat to privacy.

AUTHOR INFORMATION

P.J. Harrison is currently pursuing a graduate degree in Information Technology at UCM. She works as a scientist in a major contract pharmaceutical development company. Her research interests include security and privacy issues in health information systems.

Sam Ramanujan, Ph.D. is currently a Professor of CIS at University of Central Missouri. He has published and presented many articles in the area of software engineering, software maintenance, pedagogical issues in IT, legal issues in IT and Globalization of Information Systems.

REFERENCES

1. American Civil Liberties Union (July 22, 2008). Medical Privacy and Electronic Records. retrieved November 28, 2008 from http://www.aclu.org/privacy/medical/36069res20080722.html.
2. American Civil Liberties Union (May 30, 2003). FAQ on Government access to medical records. retrieved November 28, 2008 from http://www.aclu.org/privacy/medical/15222res20030530.html.
3. Blankenhorn, D (October 8, 2007). Today’s Debate: Privacy laws a precondition for EMR growth? ZDNet Healthcare. retrieved November 28, 2008 from http://healthcare.zdnet.com/?p=339.
4. Bright, B. (November 29, 2007). Benefits of Electronic Health Records Seen as Outweighing Privacy Risks. *The Wall Street Journal Online*. retrieved November 28, 2008 from www.wsj.com.
5. Cimino, J, Teich, J, Patel, V, Zhang, J. (1999). What is Wrong with EMR? (Panel Proposal submitted for consideration by the program committee for the 1999 Annual Symposium of American Medical Informatics Association). retrieved November 28, 2008 from http://www.docstoc.com/docs/2238706/What-is-Wrong-with-EMR.

6. Collins, T. (September 30, 2008). *Computer Weekly*.
7. Conn, J. A long-term solution: IT scarce in nursing homes, but likely key to future care. *Modern Health Care*; (November 12, 2007): page 52.
8. Department of Health and Human Services, Office of Civil Rights (Revised April 3, 2003). General overview of standards for privacy of individually identifiable health information (45 CFR Part 160 and Subparts A and E of Part 164] retrieved November 28, 2008 from http://www.hhs.gov/ocr/hipaa/.
9. DoBias, M. IT Bill Draws Concerns: Industry leery over pay, privacy, security matters. *Modern Healthcare*; July 28, 2008: page 8.
10. Former UCLA employee indicted for HIPAA violations over celbs. *Modern Healthcare*; May 5, 2008: page 4.
11. Fujitsu Computer Products of America, Inc.; Fujitsu PalmSecure and HT Systems' PatientSecure Selected by BayCare Health System to Protect Patient Confidentiality and Prevent Medical Identity Theft. *Hospital Business Week*; October 12, 2008: page 35.
12. Harris Corporation; Enterprise Intelligence Technology from Harris Corporation Plays Key Role in Nationwide Health Information Network Demonstration. *Lab Business Week*: October 12, 2008: page 959.
13. Many complaints of privacy violations not investigated. *American Health Line*; August 19, 2008.
14. NHS staff go unpunished for patient data breaches. *Pulse*; September 17, 2008: page 3.
15. Partners in Health (2008). EMR Benefits, Challenges, and Uses. retrieved November 28, 2008 from http://model.pih.org/electronic_medical_records/benefits_challenges.
16. Privacy Rights Clearinghouse. (revised September 2008). Fact Sheet 8: Medical Records Privacy. retrieved October 12, 2008 from www.privacyrights.org.
17. Stark Introduces EHR Adoption Bill. *American Health Line*; September 16, 2008.
18. State of Ohio (April 2002). *Reasons for implementing HIPAA.* retrieved November 28, 2008 from hipaa.ohio.gov/whitepapers/reasonsforimplementinghipaa.pdf.
19. Taylor, H, Ed (August 10, 2004). Two in Five Adults Keep Personal or Family Health Records and Almost Everybody Thinks This is a Good Idea: Electronic health records likely to grow rapidly. *Health Care News*; volume 4, issue 13.
20. Taylor, L. *HIPAA 101*. Intranet Journal retrieved November 28, 2008 from http://www.intranetjournal.com/articles/200211/ij_11_29_02a.html.
21. United States Department of Health and Human Services, Office of Civil Rights (last revised May 2003). OCR Privacy Brief “Summary of the HIPAA Privacy Rule. retrieved November 28, 2008 from http://www.hhs.gov/ocr/hipaa/.
22. Wang, S, et al. (2003). A Cost-Benefit Analysis of Electronic Medical Records in Primary Care. *Am J Med.* 2003;114:397– 403.

NOTES