ARTICLE

To serve and protect? Electronic health records pose challenges for privacy, autonomy and person-centered medicine

Talya Miron-Shatz MA PhD[a] and Glyn Elwyn MB BCh MSc FRCGP PhD[b]

a Founding Director, Center for Medical Decision Making, Ono Academic College, Israel; Lecturer, Marketing Department, Wharton School, University of Pennsylvania, Philadelphia, Pennsylvania, USA
b Professor of Primary Medical Care, Clinical Epidemiology Interdisciplinary Research Group, Department of Primary Care and Public Health, Cardiff University, Cardiff, UK

Abstract

This paper highlights potential challenges to privacy posed by electronic health records and proposes to increase patient involvement in maintaining the privacy of their data. Electronic health records are heavily promoted in the United States, rendering sensitive health information accessible and potentially jeopardizing patient privacy. Yet certain HIPAA regulations are consistently violated, suggesting that the Federal Government is unable to fully enforce privacy standards. On the other hand, proportionately there are few civilian complaints to the U.S. Department of Health and Human Services (HHS), implying that patients are unaware of privacy breaches, the means to report them, or both. Without permitting patient control over information, the proposed privacy system assumes that leakages will occur and offers to notify patients of breaches after the fact. This deprives patients of the right to defend their intimate details, which are more available to caretakers, employers, and insurers than ever. Our proposed solution is to render usage of patient information transparent by default, so that patients can monitor and control who is privy to what input. This will enhance patient empowerment, feeding into improved governmental control over health data.

Keywords

Computerized, confidentiality, electronic health records, HIPPA patient participation, medical records systems

Correspondence Address

Dr. Talya Miron-Shatz, 716 JHH, 3730 Walnut St., Wharton School, University of Pennsylvania, Philadelphia, PA, 19104-6340, USA. E-mail: talyam@wharton.upenn.edu

Accepted for publication: 14 May 2011

Introduction

Informing consumers of their privacy rights is required by public law. Unfortunately, consumers often need to advocate for themselves in order to receive the appropriate information. A dental consumer had the following experience. It was Mara's first visit to a new dentist's office. She was handed a packet of forms to sign. The final page asked her to acknowledge that she had received and read the Notice of Privacy Practices, but she had not received this notice. On the following visit, the receptionist came over, waving the unsigned form. Mara was a bit bewildered, she explained that she never received the notice during her first visit. The receptionist unapologetically gave her the form anyway. Had the ailment been more severe, had Mara been more dependent on this dentist, or had there been no other dental offices nearby, she may not have insisted. However, she did and the receptionist handed her a notice on the Health Insurance Portability and Accountability Act (HIPAA), enacted by the U.S. Congress in 1996.

Even when consumers know their rights, privacy violations can occur quite easily. Goldberg [1] reminds us how patients are potentially vulnerable recounting an incident where a doctor who, after leaving a clinic, logs into the EMR system and downloads the files of associates' family members. These individuals wish to sue and are supported by the HITECH Act. The illustration, however, is based on the assumption that they know their privacy has been violated, though how this would happen is unclear. For want of transparency and tracking mechanisms we claim it is hard, if not impossible, for patients to detect HIPPA and HITECH violations.

Title II of HIPAA [2] decrees that standards for dealing with health information be maintained by covered entities and lists penalties for violations. The notice "presents the information that federal law requires us to

give our patients regarding privacy practices" and continues with "Our legal duty," which is "to maintain the privacy of your health information" and "to give you this Notice about our privacy practices…." The questions and complaints page guarantees that the office will not retaliate should a patient file a complaint with them or with the U.S. Department of Health and Human Services (HHS). In Mara's instance, the lines meant for the contact officer's name, phone, fax and email were blank, rendering the suggested complaint process mere lip service.

The experience suggested that privacy protection is considered not a patient's right but an additional paperwork burden by healthcare office staff and supervisors. While the academic literature seldom addresses this issue, the popular press suggests that maintaining HIPPA regulation is laborious for physicians and administrators. The administrative procedures and extra cost surrounding the Notice have been described as a burden for providers [3]. Indeed, physicians complain of HIPAA inconveniences that range from those that are minor in nature to those that can interfere with patient care [4]. Researchers have also found that larger hospitals exhibit particularly low compliance which appears part of a general trend - this may be due to the low incentives and benefits to be gained from 100% observance, from the point of view of health care providers [5].

Though patients cannot monitor providers' adherence to privacy rules, procedural violations such as neglecting to present the HIPAA notice are commonplace. Why then would patients trust providers to maintain their privacy? Why would they trust government to enforce the privacy regulations when these are clearly violated? When a patient later grants his employers permission (or "compelled disclosure") to examine her medical records, how can he ensure that they will only view relevant details and that historical health events will not be identified and employed in a disadvantaging manner? [6].

How efficient are current means of monitoring privacy?

Nevertheless, the accelerating transition to electronic health records [7] gained impetus in 2009 when President Obama pledged that the recovery plan would invest in electronic health records and new technology would be introduced to reduce errors, reduce costs, ensure privacy, and save lives [8]. Under the new Health Information Technology for Economic and Clinical Health (HITECH) Act, which expands HIPAA's scope to electronic information, covered entities and business associates must notify individuals and the HHS Secretary of breaches [9]. Should a breach affect more than 500 individuals, prominent media outlets must also be notified. Such requirements are commendable, but notifications after the event only serve to raise concerns; patients can do little to defend themselves against the compromise of their most intimate information.

Citizens can file complaints concerning privacy and procedural breaches to the HHS [10], which operates a user-friendly website that offers information in multiple languages. Most complaints (64% in 2008 and 59% in 2009) are resolved after intake and review, indicating that the means for maintaining privacy exists, but reinforcement is sometimes lacking. The number of complaints rose from 3743 in 2003 (after HIPAA became law on April 14th) to 8526 in 2008, dropping to 7515 in 2009. Given the size of the U.S. population, one wonders whether the numbers reflect a low rate of violations or the fact that citizens are unaware of violations, not motivated to take action, or not knowledgeable about how to exercise their rights.

The premise of the brave new world of electronic health records is ensuring patient privacy. While the transition to electronic formats will indeed bring about benefits to protection of information, information ownership remains unclear [11]. While 100% secure management of personal medical information cannot be guaranteed, the adoption of measures to be taken in the case of a breach cannot replace patient control.

Increasing challenges to privacy with electronic health records

Inevitable tension exists between the needs of those delivering, regulating, and paying for healthcare and patients' needs for privacy and confidentiality [12]. As more personal data become aggregated in distributed and linked online databases [13,14], the information's whereabouts and uses may surpass the control of owners and administrators, rendering concerns over privacy breaches increasingly legitimate.

Patient and healthcare consumer control over information is already limited because Federal, State and local authorities collect, store and use personal health and behavior data such as injury, child neglect and risk of communicable disease based on public trust while unsupervised by HIPPA [15]. Patients have also lost the measure of privacy afforded by the fragmentation of paper records. In an electronic era, information is aggregated and breaches of privacy might lead to greater damage, as there is more data about the individual recorded, so that many more details can then be accessed. Maintaining patient privacy is furthered challenged as government data warehouses grow exponentially and become more linked, consisting of socioeconomic, educational, criminal, health and other records. While data warehouses are also being established in contexts such as academia and private industry, these aggregates are not expected to act in the best interest of the people whose records they manage. Indeed, patients have little choice but to accept such government-managed warehouses if they expect to enjoy

benefits like unemployment insurance and driving privileges. Similarly, warehouses are also being established by insurers, researchers and the like and privacy concerns are pertinent there too. Concerns regarding confidentiality were raised as early as the 1960s [16] when they centered on issues such as theft, damage and unauthorized access to clinics' records; they persist today [17], but now the focus is on the amount of health information that is even more readily available online.

Recommendations

The government is not oblivious to the challenges involved with using EHRs. The national coordinator for health information technology at the Department of Health and Human Services (DHHS) and the principal deputy administrator of the Centers for Medicare and Medicaid Services have recently written that, "realizing that the privacy and security of EHRs are vital, the DHHS has been working hard to safeguard privacy and security by implementing new protections contained in the HITECH legislation"[18]. Yet the most important sentinel guarding the security and privacy of health information is the individual whose privacy might be compromised. Researchers like Pfeiffer et al. [19] have suggested that for the sake of modern integrated health and for patients to assume an active role, electronic health solutions need to be user-friendly, secure and efficient. Thus, while it is the patient's responsibility to take charge of his health and protect the privacy of his data, it is the health provider's responsibility to facilitate and streamline active patient participation. While some patients, especially those who are chronically or severely ill, set little store by privacy [20], others may be less lax. Increased patient control will add to the system's maintenance of privacy.

The analysis above suggests, however, that, rather than placing additional demands on patients, healthcare records as well as data protection and tracking may need reform. The Veterans' Administration (VA), for example, acknowledges the challenges of interconnected computer systems and addresses privacy and security concerns by requiring security certification and documentation for software, as well as security training for staff [21]. Google and Microsoft, aiming for commercial benefits, advocate a model of personally-controlled health records that have intricate information-release mechanisms. Jing et al have developed, "a unified access control scheme" of virtual composite EHRs that are patient controlled. These allow one aspect of a larger patient file to be shared [22]. Notwithstanding potential trade-offs like third-party advertising and marketing strategies based on behavior, such records are supposed to revolutionize healthcare administration, offering secure storage and allowing release to providers at the patient's discretion [23]. While the possibility of security breaches exists, users have more intentional control over who sees their health information, compared with systems in which an external entity controls the data. The financial system offers an equivalent: many individuals have learned to monitor and manage online bank accounts. These models assume that the consumer is savvy enough to assert control over their health information.

Yet not every patient is likely to have his or her own health record, let alone skillfully manipulate it. A recent study [24] examined use of personal health information management systems by elderly, low-income residents of an apartment complex. The systems were available for free, as were personal assistance and access to computers with internet connections. Yet, only 13% of the 330 eligible residents used the system, and of those, almost half used it only once. A follow-up survey illustrated the challenges of introducing personally managed electronic health records to all: of the 14 residents who responded to the survey, most were satisfied with the system, shared their records with their primary care providers and /or specialists and found that the system made their meetings with providers more efficient, so that ultimately patients were in better control of their care. Acknowledging the meager participation rates, the authors conclude that the future elderly generation may be more tech-savvy and better able to manage their health records than the present generation. Still, for some, if not most, information will inevitably remain in the hands of providers, insurers and their administrators.

A potential compromise that may assist current users would be to increase confidence in existing insurance or government-based systems by expanding patient involvement in monitoring the data. Patients should gain some ability to view access records and control who gets access, which would be an improvement over the lack of agency associated with being notified of a breach after it occurs. Indeed, some have deemed such access a fundamental right and called for patient control over access to and the flow of their clinical data [25]. But how will this be carried out?

Perhaps we need to consider systems that allow existing patients the required transparency and reassurance that their data is safe. We imagine a process that allows patients to monitor, even comment on, their data and, if needs be, alert their health providers and federal agencies to problems. A paradigm shift in maintaining security and confidentiality that involves a culture of custodianship, rather than ownership, of patient data has been discussed since the 1970s [26-28]. It suggests that while health systems hold confidential information about patients, it is not the system's right to use this information as it chooses. Rather, the system needs to secure patients' consent to transfer records or data to a third party, even if it is another medical caretaker. One recommendation we adopt from the custodianship approach is that patients should have the ability to control the flow of their clinical data and to grant access to it. Similar opinions have been voiced elsewhere by medical professionals, specifically in the context of genetic information [29].

A fact well-known to decision scientists is that defaults prevail: the way systems are designed sends a clear, if implicit, message on how they should be used [30]. If the default is that information on who accesses records and for what purpose is automatically registered (audit trail), then patients and other authorized personnel should be able to review the use of their data and act accordingly if breaches occur. Likewise, for individuals external to the system like researchers, patients can actively grant – or withhold – the right to utilize whatever portion of their information they deem appropriate – to whomever they choose, barring administrative necessities. The distinction here between health providers and agents external to the system is significant; health providers have professional and moral obligations to use the available information for health care, whereas external agents are not similarly bound. Hence, allowing passive control by patients over health providers and more active control over external agents would provide a more vigilant custody of valuable and sensitive healthcare data and, as a by-product, more trustworthy electronic health records.

None of the above precludes the benefits of EHRs and the fact that progress, whether seal-proofed for privacy or not, is here. Efficient recruitment for clinical trials is but one of the benefits offered by a centralized, computerized system [31]. Another is the ability of physician practices to generate registries of patients with particular clinical attributes, such as diagnoses or medications taken, so as to implement broad-based quality improvements [32]. These benefits to individuals and to the healthcare system may, however, come with a price that patients will be unaware of until it is too late.

References

[1]. Goldberg D. Access denied: HIPAA, HITECH mandate need-to-know for retrieving EMR files. Dermatology Times. 2011.

[2]. The Health Insurance Portability and Accountability Act (HIPAA) of 1996. Pub. L. No. 104-191. Accessed January 13, 2011, http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__home/1204

[3]. Guthrie, J. (2003). Time is running out - the burdens and challenges of HIPAA compliance: A look at preemption analysis, the minimum necessary standard, and the notice of privacy practices. *Annals of Health Law* 12, 143-178.

[4]. Darves, B. (2003). From minor annoyances to treatment delays, physicians feeling fallout of HIPAA privacy law. ACP Observer.

[5]. McIntosh, M. (2007) Healthcare applications and HIPAA [2007 May 4; cited 2011 Jan 2]. Available from: http://citebm.business.illinois.edu/TWC%20Class/Project_reports_Spring2007/HIPAA/mtmcinto/McIntosh.pdf.

[6]. Rothstein, M.A. and Talbott, M.K. (2006). Compelled disclosure of health information: Protecting against the greatest potential threat to privacy. *Journal of the American Medical Association.* 295, 2882-2885.

[7]. Steinbrook, R. (2008) Personally controlled online health data: The next big thing in medical care? *New England Journal of Medicine* 258,1653-1656.

[8]. Obama, B. Remarks of President Barack Obama– as prepared for delivery address to joint session of Congress. [document on the internet]; 2009 Feb 24. Available from: http://www.whitehouse.gov/the_press_office/Remarks-of-President-Barack-Obama-Address-to-Joint-Session-of-Congress.

[9]. Health Information Technology for Economic and Clinical Health Act (HITECH). [cited: 2011 Jan 2]. Available at: http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__home/1204

[10]. U.S. Department of Health and Health Services. Enforcement data. 2009; [2011 Jan 2]. Available at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html.

[11]. Hall, M.A. and Schulman, K.A. (2009) Ownership of medical information. *Journal of the American Medical Association* 301, 1282-1284.

[12]. Gunter, T.D. and Terry, N.P. (2005). The emergence of national electronic health record architectures in the United States and Australia: Models, costs, and questions. *Journal of Medical Internet Research* 7, e3.

[13]. Rosenbaum, J.I. (1998) Privacy on the internet: whose information is it anyway. *Jurimetrics* 38, 565-568.

[14]. Organisation for Economic Co-operation and Development. The Security Economy. Washington DC: OECD Publishing; 2004. [cited: 2011 Jan 2]. Available from: http://www.oecd.org/dataoecd/14/17/16692437.pdf

[15]. Lee, L.M., Gostin, L.O. (2009) Ethical collection, storage, and use of public health data: a proposal for a national privacy protection. *Journal of the American Medical Association* 302, 82-84.

[16]. Baldwin, R.W. (1962) Confidentiality between physician and patient. *Maryland Law Review* 22 (3).

[17]. Wynia, M.K., Coughlin, S.S., Alpert, S., Cummins, D.S., Emanuel, L.L. (2001) Shared expectations for protection of identifiable health care information. *Journal of General Internal Medicine* 16, 100-111.

[18]. Blumenthal, D. and Tavenner, M. (2010) The "Meaningful Use" Regulation for Electronic Health Records. *New England Journal of Medicine* 363 (6), 501-504.

[19]. Pfeiffer, K. (2009) Future development of medical informatics from the viewpoint of health telematics. *Methods of Information in Medicine* 48, 55-61.

[20]. Walker, J., Ahern, D., Le, L.X. and Delbanco, T. (2009) Insights for internists: "I want the computer to know who I am." *Journal of General Internal Medicine* 24, 727-732.

[21]. Box, T.L., McDonnell, M., Helfrich, C.D., Jesse, R.L., Fihn, S.D. and Rumsfeld, J.S. (2010) Strategies from a nationwide health information technology implementation: The VA CART STORY. *Journal of General Internal Medicine* 25, 72-76.

[22]. Jing, J., Ahn, G.J., Hu, H., Covington, M.J. et al. (2011) Patient-centric authorization framework for electronic healthcare services. *Computers & Security*. 30, 116-127.

[23]. Mandl, K.D. and Kohane, I.S. (2008) Tectonic shifts in the health information economy. *New England Journal of Medicine* 358, 1732-1737.

[24]. Kim, E., Stolyar, A., Lober, W.B. et al. (2009) Challenges to using an electronic personal health record by a low-income elderly population. *Journal of Medical Internet Research* 11, e44.

[25]. Wiljer, D., Urowitz, E.A., DeLenardo, C. et al. (2008) Patient accessible electronic health records: exploring recommendations for successful implementation strategies. *Journal of Medical Internet Research* 10, e34.

[26]. Acheson, H.W.K (1974). Confidentiality in general practice. *Journal of the Royal College of General Practitioners* 24, 194-195.
[27]. Winfried, E.K. (1995) A paradigm for user-defined security policies. Proceedings of the 14th Symposium on Reliable Distributed Systems. pp135–144.
[28]. Kenny, D.J. (1982). Confidentiality: the confusion continues. *Journal of Medical Ethics* 8, 9-11.
[29]. Patterson, A.R., Robinson, L.D., Naftalis, E.Z., Haley, B.B. and Tomlinson, G.E. (2005). Custodianship of genetic information: clinical challenges and professional responsibility. *Journal of Clinical Oncology* 23, 2100-2104.
[30]. Thaler, R.H. and Sunstein, C.R. (2008). Nudge: Improving Decisions about Health, Wealth and Happiness. New Haven (CT): Yale University Press
[31]. Thadani, S.R., Weng, C., Bigger, J.T., Ennever, J.F. and Wajngurt, D. (2009). Electronic screening improves efficiency in clinical trial recruitment. *Journal of the American Medical Informatics Association* 16, 869-873.
[32]. Wright, A., McGlinchey, E.A., Poon, E.G., Jenter, C.A., Bates, D.W. and Simon, S.R. (2009) Ability to generate patient registries among practices with and without electronic health records. *Journal of Medical Internet Research* 11, e31.