Bioethics and Information Technology

Safeguarding Confidentiality in Electronic Health Records

AKHIL SHENOY and JACOB M. APPEL

Abstract: Electronic health records (EHRs) offer significant advantages over paper charts, such as ease of portability, facilitated communication, and a decreased risk of medical errors; however, important ethical concerns related to patient confidentiality remain. Although legal protections have been implemented, in practice, EHRs may be still prone to breaches that threaten patient privacy. Potential safeguards are essential, and have been implemented especially in sensitive areas such as mental illness, substance abuse, and sexual health. Features of one institutional model are described that may illustrate the efforts to both ensure adequate transparency and ensure patient confidentiality. Trust and the therapeutic alliance are critical to the provider–patient relationship and quality healthcare services. All of the benefits of an EHR are only possible if patients retain confidence in the security and accuracy of their medical records.

Keywords: electronic health records; EHR; EMR; ethics; confidentiality; privacy

Electronic Health Records (EHRs) and Patient Confidentiality

EHRs offer an opportunity to improve patient care by making health information readily available to a broad spectrum of providers, and by enabling these providers to use such data in novel ways. Among the significant advantages of EHRs are ease of portability, facilitated communication among healthcare professionals, and a decreased risk of medical errors through systematized medication and allergy reviews. In the future, the possibility also exists for an interoperable national system of medical charts that would make a patient's entire healthcare record available to first-line responders in emergencies. A health record that is accurate, up to date, and available when the patient is in need of medical attention could improve patient care across different settings. Moreover, EHR data can potentially generate new insight into disease, which can benefit all patients. At the same time, the mass storage and easy relay of sensitive health information raises significant ethical concerns related to confidentiality for both patients and their physicians. We will discuss these challenges and offer possible solutions.

Ethical and Legal Issues

Confidentiality is among the core values of ethical medical practice, dating back to at least the Hippocratic Oath. This principle has been incorporated internationally into the canons of professional organizations, and in legal statutes such as the Data Protection Act of 1998 in the United Kingdom and the Health Insurance Portability and Accountability Act (HIPAA) of 1996 in the United States, which imposes criminal penalties at the federal level for the impermissible release of patient data. Concomitantly, the American legal system has developed rules of "physician–patient privilege" and "psychotherapist–patient privilege" to shield physicians from being compelled to testify to their patients' secrets in court. These safeguards have historically been justified on the grounds that patients will not share personal health information (PHI) essential for appropriate care—especially in sensitive areas such as mental illness, substance abuse,

Cambridge Quarterly of Healthcare Ethics (2017), **26**, 337–341.

doi:10.1017/S0963180116000931

and sexual health—unless they can be certain that these secrets will remain between themselves and their healthcare providers. Trust and the therapeutic alliance it generates are central to the provider–patient relationship. Although physicians may breach confidentiality in certain narrowly circumscribed areas related to public safety, such as the reporting of communicable disease and child abuse, and may additionally disclose patient information to prevent suicide or violence, such as through so-called "*Tarasoff* duties" to warn third parties of, and protect them from, danger, the prevailing legal default and ethical norm in Western nations both strongly favor the preservation of patient confidence in the absence of compelling grounds to act otherwise.

The information contained in the EHR must be accessible to multiple users in order to confer its benefits. Busy group practices require patients to be seen by different providers and demand open access to the chart by any covering physician or nurse. For billing and administrative purposes, support staff must also have some access to the chart. In contrast to the pristine historical ideal of a single physician being the only party privy to a patient's health information, the EHR raises both the risk of intended and unintended views of PHI. These include three distinct forms of potential access that threaten patient privacy. First, EHRs are subject to "inside attacks" in which legitimate users of the record take advantage of their access to view data for purposes other than for providing patient care.[1] These uses may range from the satisfaction of personal curiosity through the generation of gossip, to (at the extreme) the sale of PHI for pecuniary gain or other criminal enterprises.[2] Whereas such a risk also does exist with paper medical records, the advent of EHRs increases exponentially the number of providers who have potential access to patient records. Second, EHRs, most of which are web-based, are subject to security breaches from outside the system. Such breaches might include a healthcare professional losing a laptop or thumb drive containing PHI on thousands of patients or an orchestrated attack by international hackers that might breach the security of millions of patients within an intraoperative database. These breaches have already occurred on a mass scale in the banking and consumer sectors, and are beginning to occur in healthcare.[3] Third, even the legitimate use of the electronic medical record (EMR) by providers for appropriate patient care raises ethical concerns. Some patients may simply not want their dermatologist to know their mental health history, or a woman may not want her pharmacist to learn that she has had an abortion. Some patients may even fear, possibly with justification, that a prior psychiatric diagnosis will compromise their workup for a current medical condition. Although patients may implicitly or explicitly consent to such comprehensive access, the degree to which they fully understand the potential consequences of this consent, including the risk of security breaches and other implications for privacy, remains unclear. Such incidental and unintended revelations in the course of legitimate use are likely the most frequent of the risks to patient confidentiality.

Concerns regarding the confidentiality of the EHR are of particular significance to psychiatric providers and their patients. The psychiatric record often combines data related to the patient's present symptoms, with a descriptive narrative of the patient's life experience, including sensitive details of psychological trauma, domestic violence, incarceration, sexual encounters, and substance abuse. Much of this information is of

great value to a therapist, but not always of clinical use to many other medical providers. The stigma attached to mental healthcare among some individuals and in certain cultural communities even leads some patients to avoid using their insurance for psychiatric care in order to protect their privacy. Patients with a documented prior history of suicidal ideations and behavior may avoid medical care for fear that they will be involuntarily hospitalized based on their past actions, rather than their current psychiatric needs. Some mental health providers have already resorted to makeshift measures to protect patient confidentiality in the EHR era, such as keeping psychotherapy notes sequestered from the medical chart, to be sent to third parties only with the patients' expressed consent.[4] Other psychotherapists choose to not keep any records at all, for fear that this material can be ordered disclosed by court subpoena, although failure to keep an adequate medical record can leave the provider vulnerable to charges of negligence.[5] Mental health professionals are placed in the difficult position of protecting their patients' privacy while also complying with the complex documentation requirements of the modern medical practice.

Potential Safeguards

Several different methods of securing EHRs can foster patient confidentiality. A first set of safeguards involve soft barriers or stops designed to remind providers to engage in ethical and appropriate use of the medical record. In addition to passwords or key cards, these might include "break the glass" (which draws its name from breaking the glass to pull a fire alarm) reminders that ask physicians to affirm their right to access sensitive material in the EHR before they do so.[6] Such soft stops may give well-intentioned providers pause, and afford protections at the margins; however, they are unlikely to deter determined malefactors.

A second set of safeguards are those that detect breaches after the fact and then seek to sanction those individuals responsible for the breach.[7] At present, these may include systems that check to see whether providers who do "break the glass" have done so as part of the treatment team, as well as other efforts to track inappropriate access, often in the context of patients likely to be targeted for breaches, such as hospital employees and celebrities. The institutions use audit logs as evidence to punish the employee, which to some degree, can prove a deterrent. However, as multiple recent episodes of hospital employees accessing the medical records of celebrities have demonstrated, this deterrent is not completely effective.[8] From a practical standpoint, post-breach punishment does little to protect patients. For example, if I am a pharmacist at a hospital and I access an interoperable system to look up my future son-in-law's EHR at another hospital, and I am caught by a surveillance algorithm, all the system can do is punish me; it cannot wipe clean my knowledge of my potential son-in-law's addiction or psychiatric histories. Moreover, terminating me in such a situation may compound, rather than ameliorate, the damage to the victim, who will now have faced both a security breach and the firing of a relative. Employees who must leave their station for an emergency without logging out leaving sensitive information exposed for a family member to view can also raise concerns about responsibility to protect the record. Clearly, after-the-fact interventions have significant drawbacks.

A third set of safeguards, which is generally both the most burdensome and the most effective, is that which

create "hard stops" to access before breach occurs. These may include sequestering portions of the medical records, such as psychiatric notes, from all but a small segment of providers. Patients may prefer this method of having specific providers have pre-allowed access to certain parts of the record.[9] Some institutions permit patients to interact directly with their health record, creating options for them to record, delete and edit information. Others have experimented with registering VIP patients under aliases and releasing these identities on a need-to-know basis. In theory, hospitals might develop EHRs that fade from view over time, but retain information invisibly for forensic purposes. However, each increased barrier to access results in a parallel decrease in the availability and hence the advantages of an EHR.

One Institutional Model

Protecting confidentiality in the EHR era requires the collaboration of both patients and providers. A systematic commitment to such protections at the institutional level is also essential.

Our institution uses a combination of soft, hard, and retrospective stops to safeguard patient confidentiality. Access to our EHR requires a password; a "break the glass" function asks providers to pause before accessing the records of sensitive or high profile patients, including those treated for psychiatric illness. Our institutional culture also encourages psychiatrists and other physicians to reflect carefully before documenting sensitive, nonessential information in the EHR, and increasingly encourages providers to make patients aware of sensitive material included in their records. At present patients can review their own problem lists and message their provider if they see a diagnosis or problem with which they disagree. Patients are informed that providers will be communicating their findings to other physicians. A "MyChart" function of our system allows patients to access their own EHR and increasingly will allow patients to add their own data. The question about how the patient can share this information with different providers will still need to be answered.

Our institution has developed a system of "nesting" sensitive information so that, for example, psychiatric records can be shielded from nonpsychiatric providers. Psychiatric notes written in the internal medicine clinic can be viewed only when signing into the psychiatric domain and only internists working within this clinic have this access. It is now the default in our faculty private practice for patient problem lists and medication lists to be transparent to other providers in our system. Patients can then choose different options for their psychiatric record: completely opaque, medication lists exposed, medication lists and problem lists exposed, or completely open. In our experience, the majority of patients seeing private psychiatrists in the faculty practice are willing to share their medication history in the general medical record. As we practice this approach, we will see if this is the best model to carry forward.

Most hospitals have a specially designated HIPAA or privacy information compliance officer who reviews access to sensitive and high profile charts. Those found to have accessed the record inappropriately are either given one warning or, if the breach occurs for personal gain, are systematically terminated. These information and compliance officers may also be charged with developing prophylactic policies to prevent future breaches.

Conclusions

EMRs have vast potential to improve patient care. In the future, patients may

be able to share real time data through mood trackers, sleep sensors, and activity logs, which will enable their healthcare providers to tailor management to these results. As their patient health record (PHR) integrates with the EHR, we may see patients adding substantially to their own health records. This ability could prove extremely helpful in the monitoring and treatment of chronic illnesses such as diabetes, hypertension, and psychiatric illnesses. For example, a tracker might detect a patient's poor sleep for several days in a row and be able to inform a psychiatrist that a patient with a diagnosis of bipolar disorder may be slipping into mania. Sudden, profound altercations in self-reported mood could prompt a provider to reach out to a depressed patient, preventing further deterioration or even self-harm. As patients review their records they could correct mistakes and update medication lists. Prescription monitoring could be linked directly to the patient's medical record and give healthcare provider feedback on completion and timeliness of refills. Improving the quality of the patient's database will help the physician engender a new trust in the knowledge of the patient to help treat that patient correctly. EHRs also hold the promise to provide benefits that transcend the acute care of individual patients. Data mining of EHRs, for example, may be the future of clinical health research. All of these benefits are only possible if patients retain confidence in the security and accuracy of their medical records.

Notes

1. Barrows RC, Clayton PD. Privacy, confidentiality and electronic medical records. *Journal of the American Medical Association* 1996;3: 139–48.
2. Mearian, L. Update: Hacker puts 9.3M U.S. patient records up for sale. available at http://www.computerworld.com/article/3088907/security/hacker-selling-655-000-patient-records-from-3-hacked-healthcare-organizations.html (last accessed 28 June 2016).
3. Akpan N. Has health care hacking become an epidemic? March 23, 2016; available at http://www.pbs.org/newshour/updates/has-health-care-hacking-become-an-epidemic (last accessed 29 Nov 2016).
4. DeLettre JL, Sobell LC. Keeping psychotherapy notes separate from the patient record. *Clinical Psychology and Psychotherapy* 2010; 17(2):160–3.
5. New York Education Law 6530(32)
6. Genes N, Appel JM. Ethics of data sequestration in electronic health records. *Cambridge Quarterly of Healthcare Ethics* 2013;22(4):365–72.
7. Hersh WR. The electronic medical record: Promises and problems. *Journal of the American Society of Information Science* 1995;46(10):772–6.
8. Hennessy-Fiske M. UCLA hospitals to pay $865,500 for breaches of celebrities' privacy. *Los Angeles Times*, July 8, 2011.
9. Caine K, Hanania R. Patients want granular privacy control over health information in electronic medical records, *Journal of the American Medical Informatics Association* 2013;20:7–15.