Special Section: Open Forum

Ethics of Data Sequestration in Electronic Health Records

NICHOLAS GENES and JACOB APPEL

Electronic Health Records and Risks

Adoption of electronic health records (EHRs) has risen dramatically in recent years.[1] This phenomenon is due in part to factors such as federal incentives for adopting EHRs, the advantages of EHRs over paper charts, and an effort to counteract an increasing fragmentation of care, driven by disparate specialties' management of an aging population.

EHRs offer several advantages over paper records. Multiple providers across an institution can simultaneously access or add content to an electronic chart, which is useful in a hospital setting. Providers can easily review a patient's up-to-date medical history, past visits, medication lists, and test results without a trip to the medical records office or a fax from a prior caregiver.

After implementing EHRs, several studies posit a reduction in medical errors and unnecessary redundancies of care, or, in other cases, reduced costs and improved efficiency[2,3,4] (although other studies show more ambiguous or contradictory results[5]). A further benefit becomes apparent as more of the U.S. population's health information is organized and entered into EHRs: analysis of aggregated, deidentified data promises to identify healthcare disparities,[6] aid biosurveillance efforts,[7] and make medically important new associations among demographics, diseases, and adverse drug reactions.[8]

EHRs also hold promise for enhanced safety and security. Because every provider's orders and activities are logged in the chart, investigators or administrators can reconstruct patient care events, potentially benefiting quality improvement initiatives or research into physician behaviors. As for security, with paper charts, it's impossible to know who has viewed a patient's results, or how many times a chart has been copied, mailed, or faxed. Electronic charts have audit logs, and some systems are equipped to detect anomalous activity; unlike paper charts, unauthorized access can be tracked, and administrators can be notified when a user is viewing charts outside his or her normal role.[9]

Despite these benefits, there are risks to moving health data into an electronic realm—including risks to patient data security and privacy.

The primary security concern is that EHRs lower the barriers to unauthorized viewing of data. Access that previously required physical proximity to a chart, or an accomplice with access to a fax machine, can now be achieved via remote login and a search of the patient database,[10] or from records downloaded to an unencrypted laptop, subsequently lost.[11] In several well-publicized cases,[12] curious

Cambridge Quarterly of Healthcare Ethics (2013), **22**, 365–372.

doi:10.1017/S0963180113000212

hospital employees have deviated from their proscribed EHR functions to view data from hospitalized celebrities.

As health information exchanges spread and the full potential of an interoperable healthcare system comes closer to fruition, more providers will likely need access to a regional or nationwide database of medical records; thus the potential for security breaches is significant. The lower barrier to access also makes electronic health records vulnerable to hackers or cyberterrorists, on a scale that was impossible with paper records.[13] Besides the risk of stealing health data or credit and social security information, it has been suggested that attackers could cripple healthcare operations by silently altering a fraction of old patient data, throwing care plans and relationships into doubt.[14]

Beyond security, however, EHRs represent a risk to privacy—the patient's determination of how much data can be communicated to others. Patients may feel uncomfortable when even authorized providers gain access to certain elements of their history or test results.

One scenario in which a privacy violation could arise is in the emergency department (ED), when an employee becomes a patient after an on-the-job injury. Suddenly, in the context of caring for a colleague and acquaintance, the ED doctor reviewing the employee's electronic record might learn, for example, of a history of drug use. This information is not relevant to the reason for visit and is more than the employee wanted his colleague to know about him.

Health Data Sequestration

To assuage the concerns of patients and privacy advocates, and to promote the appearance of high-security standards, vendors of electronic health systems have turned to an old concept: sequestering health data.

Sequestration of sensitive patient information dates back to the paper chart era, when certain pages or notes from a chart were physically separated from the main chart and treated with additional scrutiny.[15] Sequestration has traditionally been justified by beneficence: the notion (which has some support) that patients would be more likely to seek care if potentially stigmatizing history or results were kept out of the common chart, hidden from regular providers. Data on this phenomenon, beyond surveys, is obviously hard to come by—even if it's only anecdotally true, proponents argue that there are clear benefits to sequestration.[16,17]

However, in the paper chart era, sequestration was not as much a policy decision as a reflection of the fragmented nature of healthcare delivery; many patients who saw multiple specialists likely had some elements of their charts sequestered in filing cabinets across offices. As EHRs gain adoption and health information exchange capabilities grow, providers that patients might have preferred to keep isolated (or to keep in the dark) can now discover one another and communicate about prior care.

With time, as the breadth and depth of electronic charts grow, specialists and new physicians will be privy to old, likely irrelevant, and potentially stigmatizing information—unless sequestration is employed. If a teenage patient's therapy for a chlamydia infection (after a night of indiscretion) is entered into an EHR in 2012, should it be retrievable to an orthopedist managing that same patient's hip fracture half a century later? Sequestration seems ideal for health data that is unlikely to affect future care but could likely serve to embarrass patients.

Currently, EHR vendors offer several forms of sequestration[18] to healthcare institutions or patients that request it:

- Data that patients or institutions deem sensitive can be hidden behind a break-the-glass warning in a pop-up window. For instance, if a hospital deems all HIV test results as sensitive, providers can still access these sections of a chart in the course of care, by reentering their login information. However, the warning may dissuade their inquiry, and their activity triggers a privacy officer's audit.
- The entire patient record can be deemed as sensitive. This option is selected by hospitals on behalf of VIP patients or patients who are employees, as an additional disincentive to curious EHR users who are not involved with the patient's care.
- Sensitive data can be hidden, depending on the user's role. A physical therapist, for instance, would simply not see a list of his patient's psychiatric visits or notes sandwiched between physical therapy (PT) sessions. Keeping sensitive parts of the chart invisible to certain users would make it seem like this patient only had encounters with PT.

Pop-up alerts requiring users to reenter their login credentials seem like a benign enough intervention, although well-meaning administrators have burdened EHRs with so many similar warnings that usability experts have expressed concern about "alert fatigue" (when providers are confronted with so many messages that they simply stop paying attention to all of them, ignoring the potentially useful ones as they try to resume the task at hand).[19] There is also something to be said for minimizing workflow disruptions in already chaotic healthcare environments; interruptions in the emergency department, for instance, likely contribute to errors in decisionmaking.[20]

But sequestering health data by hiding it—keeping providers completely oblivious to certain types of EHR notes, test results, or visits—is the most concerning method of sequestration.

Extrapolating from current trends in search engines and social networks, one might imagine a not-too-distant future when "dynamic sequestration" electronically hides data from clinicians based on rules, circumstances, and predefined patient preferences. In this way, the patient's record need not disclose anything potentially uncomfortable, and (assuming the conditions are set properly) no clinically relevant information is kept hidden from the provider. Moreover, if a patient's circumstances change, information could be revealed to those that need to know it. For instance, if a patient presents to the emergency department with altered mentation, his or her previously hidden psychiatric medications would be visible to emergency physicians accessing the chart. Perhaps we could imagine a system smart enough to keep the psychiatric medications hidden if the emergency visit was an innocuous ankle sprain.

In this hypothetical future with dynamic, intelligent sequestration, patients could move freely through the healthcare system, comfortable in the knowledge that information they'd prefer not to disclose would remain hidden, unless their safety was at stake.

Is this a state of affairs worth pursuing? We argue it is not.

The Case against Sequestration

There are undoubtedly cases in which, in the course of routine care, a physician learned something from an electronic health record that made a patient uncomfortable. If this knowledge didn't affect the physician's care plan, the discovery is regrettable. If the physician disclosed what was learned to uninvolved parties, it is illegal.

Calling such a discovery regrettable is not meant to diminish this potential violation, but it must be noted that revelation of private data in an electronic health record does occur within the context of the physician-patient relationship—a unique and protected form of communication.

Although the disclosures currently associated with a physician-patient relationship may be uncomfortable, it must be noted that erecting barriers to accessing a patient's full record is not without risk. Indeed, we argue that the risks of sequestration outweigh the benefits.

The first and most obvious risk is that sequestered data may have a bearing on a patient's care; a provider cannot act on information that is hidden.

Related risks include the time, expense, and potential harm in repeating testing to establish a diagnosis that had been hidden from the provider. Time is valuable for both the patient (disease states can progress in the hours or days that a provider is in the dark) and the healthcare system (extra time directed at one patient may limit opportunities to apply care elsewhere). Attempts at estimating the time physicians spend looking for health data at other institutions have been made and could be extrapolated to sequestration scenarios to suggest a significant burden.[21,22]

Take, for example, one scenario that sequestration technology makes distressingly possible: an obtunded patient is brought to the ED whose recent psychiatric hospitalization and medication list is sequestered and invisible to the ED provider, as a matter of hospital policy. The patient doesn't receive the appropriate therapy for his unusual overdose in a timely fashion; the ED physician instead undertakes a costly diagnostic workup and spends extra time with this unnecessarily complex case at the expense of other patients in the department.

Although it is difficult to estimate how common sequestration might cause wasteful or dangerous scenarios like this, we know that health information exchange and efficient data sharing has been shown to reduce costs across networks;[23] therefore we can infer that hiding data increases costs.

Another finite resource is the capabilities of the EHRs. Although some aspects of EHR adoption in modern healthcare are still debated, it's widely agreed that EHRs can lead to improvements with regards to usability, efficiency, security, and patient outcomes. Resources devoted to creating and maintaining sequestration are resources that could instead be used for more tangible benefits.

Furthermore, sequestering data introduces new, vendor- and site-specific standards at a time when the industry has been moving toward standardized protocols and interoperability.[24] Accommodating various sequestration models adds another obstacle to interoperability, delaying the anticipated benefits for questionable gains.

Even limited efforts to wall off portions of the chart may prove deleterious. Requiring providers to break the glass, for instance, is certainly irksome; more concerning, one can easily imagine that the process might contribute to alert fatigue or might disrupt the provider's train of thought in a busy emergency room or outpatient clinic.

In addition, sequestration generates an additional and unnecessary barrier to creating an interoperable medical records system. No standardization or consensus exists among vendors, institutions, or even privacy experts as to which aspects of the chart, if any, are suitable for sequestration. Similarly, variability exists among the mechanisms of sequestration used by vendors. If an interoperable system were superimposed on the current patchwork of sequestered records, the result would likely compromise care in two distinct ways: First, those accessing medical records from another institution might not realize that they do not have access to as much of the record as they do at their home institutions, which can misinform medical decisions. Second, patients might assume that more of their record was available to such providers than actually was visible, generating dangerous misunderstandings. Even if these dangers could be surmounted, such as through various pop-up warnings, sequestration mechanisms add yet another burden to the already-daunting challenge of creating an interoperable health system.

Furthermore, sequestration may create the illusion of security, rather than actual security. The most serious threats to medical privacy are unlikely to come from incidental or even unscrupulous access by medical providers, but from outside interests who hack into the medical record system or maliciously alter data. Anyone who can enter the system illicitly, in this manner, will likely also be capable of circumventing any internal sequestration mechanism with ease. The authors are reminded of past efforts to secure oceangoing liners, such as the Titanic, by erecting barriers between various holds of the ships. In case of hull breach, these barriers were to keep the ships from sinking. Needless to say, this method has not always proven effective; stronger outer hulls are a smarter approach. Similarly, the American medical record system requires strong security to prevent unwelcome third parties from accessing or damaging the data. What it assuredly does not need are internal walls that prevent physicians from helping their patients.

These risks of sequestration—the barriers to efficient care and to interoperability and the illusion of security, are difficult to quantify or study, but they are real. We have experienced many of these risks, in the course of our clinical duties or in discussing EHR implementation and usability priorities with vendor representatives. These risks seem at least as worthy of consideration as the purported benefits of sequestration.

Finally, there is the problem of simply discussing sequestration with patients. In much of modern medicine, when a patient is confronted with a therapy or procedure, providers discuss the risks and benefits with the patient and obtain consent before proceeding. Obtaining consent from patients for health data sequestration would be valuable; we could correct the often-encountered, mistaken notion that sequestered data is somehow more secure from cyberattack, or cannot be discovered in legal proceedings.

Yet we are not aware of any EHR that allows patients to adjust their privacy settings—they are unable to specify what data is visible to which providers (unlike the privacy controls available in popular social network software). Every physician who logs into an EHR is warned about the penalties of violating patient privacy, but patients are not, to our knowledge, warned about the risks of concealing sensitive data from their caregivers.

Advocates for sequestration argue that some elements of a patient's medical history are of so little relevance to any likely aspects of present-day care that they need not be accessible to all providers.[25] Rothstein offers two examples of information that supposedly lacks such relevance: "a decades-old report of domestic violence at the hands of a former partner that did not result in serious physical harm" and "a decades-old series of negative test results for various sexually transmitted diseases ordered after an ill-advised and not repeated sexual dalliance."[26] Yet these extreme examples reveal the inherent dangers in any scheme of sequestration. First, it is not at all clear that even these cases might not impact present-day care. For instance, if a patient who previously tested negative for sexually transmitted diseases suddenly has a positive result on a hospital syphilis screening test (such tests are routine for many psychiatric evaluations), a comparison with the previous results could shed light on the date of exposure and rule out a genetic or congenital variation that might have skewed the laboratory results. Similarly, if a violent former partner returned to a patient's life unexpectedly, possibly after release from an unrelated prison offense, a conscientious physician would assuredly want to know this history in order to help protect her patient. Phrased more generally, such remote data is only irrelevant until it isn't. Second, any process for excluding such data will likely prove highly subjective and will therefore be either over- or underinclusive. Do we ask the patient whether he wants a specific piece of data sequestered? If we do, how do we distinguish the patient who has had only one remote dalliance from the patient who remains sexually incautious but lies about it? One of the key reasons physicians maintain medical records is precisely because many patients either are unreliable historians, fail to mention crucial elements of a medical history, or, in some cases, are overtly dishonest. In short, sequestration always runs some risk of compromising care.

Yet the drawbacks of sequestration extend beyond culling particular tidbits of information from the medical record. The culture of sequestration reinforces many of the very social prejudices that modern medicine strives to combat. By telling patients that their mental health records are off-limits to their primary care providers, not only do we deter these doctors from looking for changes in a patient's psychiatric health, but we also suggest to patients that there is something different or even shameful about receiving psychiatric services. What better way to stigmatize a whole swath of conditions—from substance dependence to STDs to therapeutic abortions—than by telling patients that these conditions are so compromising that even their own physicians are not allowed to know of them? Compounding matters, this process then becomes self-perpetuating: the more we keep certain aspects of care out of the general record, the more our culture will view those aspects of care as items that *should* be kept out of the general record.

The gravest threat posed by sequestration, however, is to the open and trust-based nature of the physician-patient relationship. Quality medical care has long been grounded on what is termed the "Hippocratic bargain." When a patient consults a physician, either for a life-or-death illness or for a minor injury, the patient implicitly agrees to expose the most private aspects of his body and/or mind to the inspection of the caregiver. In return, the doctor is ethically obligated to use this information to serve the patient's interests and wishes, maintaining confidentiality in all but a few narrowly circumscribed situations. A crucial aspect of that Hippocratic relationship is the ability of the physician to draw on the knowledge and expertise of colleagues, and to share that private information, if necessary, with other providers who stand behind the same Hippocratic wall and are bound by the same fiduciary duties. Sequestration undermines the foundations of this mutually beneficial understanding.

When administrators and vendors block access to portions of the chart, or allow patients to pick and choose which tests or visits can be hidden, the doctor-patient relationship erodes. Sequestration encourages physicians to retreat further into a box of specialization, viewing their patients through a narrower perspective, focusing on the trees and ignoring the forest. How can they focus on the forest, after all, if they are not permitted to see its map? In turn, patients will become less trusting of providers and will inevitably keep more information to themselves, as they're prompted to decide which symptom to share with which specialist, so that it does not enter their general medical record. Ultimately, patients may even seek or receive less care, creating the very situation sequestration was intended to prevent.

Notes

1. Jha AK, Burke MF, DesRoches C, Joshi MS, Kralovec PD, Campbell EG, et al. Progress toward meaningful use: Hospitals' adoption of electronic health records. *American Journal of Managed Care* 2011 Dec;17(12 Spec No.):SP117–24.
2. Baumlin KM, Shapiro JS, Weiner C, Gottlieb B, Chawla N, Richardson LD. Clinical information system and process redesign improves emergency department efficiency. *Joint Commission Journal of Quality and Patient Safety* 2010 Apr;36(4):179–85.
3. Silow-Carroll S, Edwards JN, Rodin D. Using electronic health records to improve quality and efficiency: The experiences of leading hospitals. *Issue Brief (Commonwealth Fund)* 2012 Jul;17:1–40.
4. Zlabek JA, Wickus JW, Mathiason MA. Early cost and safety benefits of an inpatient electronic health record. *Journal of the American Medical Informatics Association* 2011 Mar–Apr;18(2):169–72.
5. Jones SS, Adams JL, Schneider EC, Ringel JS, McGlynn EA. Electronic health record adoption and quality improvement in US hospitals. *American Journal of Managed Care* 2010 Dec;16(12 Suppl HIT):SP64–71.
6. Pantazos K, Lauesen S, Lippert S. De-identifying an EHR database—anonymity, correctness and readability of the medical record. *Studies in Health Technology and Informatics* 2011;169:862–6.
7. Rea S, Pathak J, Savova G, Oniki TA, Westberg L, Beebe CE, et al. Building a robust, scalable and standards-driven infrastructure for secondary use of EHR data: The SHARPn project. *Journal of Biomedical Informatics* 2012 Aug;45(4):763–71.
8. Churchill R, Lorence D, Richards M. Proposed model for ONCHIT pre-case biosurveillance using multiple array sensing and non-invasive data capture. *Journal of Medical Systems* 2010 Aug;34(4):695–700.
9. Boxwala AA, Kim J, Grillo JM, Ohno-Machado L. Using statistical and machine learning to help institutions detect suspicious access to electronic health records. *Journal of the American Medical Informatics Association* 2011 Jul–Aug;18(4):498–505.
10. Mohammad Y, Stergioulas L. Building an information security strategy for EHR: Guidelines for assessing the current situation. *Conference Proceedings of the IEEE Engineering in Medicine & Biology Society* 2010:3919–22.
11. Kowalczyk L. MGH to pay 1m to settle privacy case. *Boston Globe* 2011 Feb 25.
12. Lambert B, Schweber N. Hospital workers punished for peeking at Clooney file. *New York Times* 2007 Oct 10.
13. Losefsky W. The efficacy of best practices in recovery from cyberattacks. *Journal of Healthcare Protection Management* 2012;28(1):104–7.
14. Haugh R. Cyber terror. *Hospitals & Health Networks* 2003 Jun;77(6):60–4, 2.
15. Lamberg L. Confidentiality and privacy of electronic medical records: Psychiatrists explore risks of the "information age." *JAMA* 2001 Jun 27;285(24):3075–6.
16. See note 15, Lamberg 2001.
17. Salomon RM, Blackford JU, Rosenbloom ST, Seidel S, Clayton EW, Dilts DM, et al. Openness of patients' reporting with use of electronic records: Psychiatric clinicians' views. *Journal of the American Medical Informatics Association* 2010 Jan–Feb;17(1):54–60.
18. Miaoulis W. Sequestering EHR data in IT systems. *Journal of American Health Information Management Association* 2009 May;80(5):50–1.
19. Weingart SN, Simchowitz B, Padolsky H, Isaac T, Seger AC, Massagli M, et al. An empirical model to estimate the potential impact of medication safety alerts on patient safety, health care utilization, and cost in ambulatory care. *Archives of Internal Medicine* 2009 Sept 14;169(16):1465–73.

20. Chisolm DJ, Purnell TS, Cohen DM, McAlearney AS. Clinician perceptions of an electronic medical record during the first year of implementaton in emergency services. *Pediatric Emergency Care* 2010 Feb;26(2):107–10.
21. Shapiro JS. Evaluating public health uses of health information exchange. *Journal of Biomedical Informatics* 2007 Dec;40(6 Suppl):S46–9.
22. Johnson KB, Unertl KM, Chen Q, Lorenzi NM, Nian H, Bailey J, et al. Health information exchange usage in emergency departments and clinics: The who, what, and why. *Journal of the American Medical Informatics Association* 2011 Sep–Oct;18(5):690–7.
23. Frisse ME, Johnson KB, Nian H, Davison CL, Gadd CS, Unertl KM, et al. The financial impact of health information exchange on emergency department care. *Journal of the American Medical Informatics Association* 2012 May–Jun;19(3):328–33.
24. Blumenthal D. Implementation of the federal health information technology initiative. *New England Journal of Medicine* 2011 Dec 22;365(25):2426–31.
25. Rothstein MA. The Hippocratic bargain and health information technology. *Journal of Law, Medicine & Ethics* 2010 Spring;38(1):7–13.
26. See note 25, Rothstein 2010, at 5.