Published in final edited form as:

Health Aff (Millwood). 2009 ; 28(2): 447–449. doi:10.1377/hlthaff.28.2.447.

Protecting Patients in Health Information Exchange: Defense of The HIPAA Privacy Rule

Clement J McDonald, MD

Lister Hill Center, National Library of Medicine, National Institutes of Health

Abstract

Regional health information organizations (RHIOs) rapidly integrate and deliver patient information to clinicians from multiple independent care organizations. By providing such information they will reduce the care costs and improve care safety. Special concerns about privacy arise as these regional systems connect nationally. We should add special barriers beyond the protections of HIPAA to protect against surprises at the national level. At the local level, we should remain within HIPAA rules because the application of additional barriers within RHIO access would interfere with efficient and safe care.

Health information exchanges are networks that facilitate electronic access to health data from independent care organizations at the point of care, in order to remove delays, reduce costs, and improve the safety of patient care. Health information exchanges variously provide information about prescribed medications, laboratory test results, radiology reports, operative notes, electrocardiogram reports and other test results. However, no system provides everything that could benefit care.

Health Information exchanges that now exist cover geographic regions of modest size e.g., portions of states (the Indianapolis Network for Primary Care in Central Indiana)¹ Memphis in western Tennessee and or special populations e.g. pediatric, in the Electronic Child Network of Ontario Canada. Because they are focused on the care organizations in a region, they are called Regional Health Information Organizations (RHIOs). Some of the current RHIOs provide access to data for millions of patients, but populations of this size are not by themselves a new or worrisome factor. Many of large private health care organizations carry more information about larger numbers of individuals within their medical record system than any RHIO. Reassuringly, neither these large private care organizations nor the RHIOs have been prone to privacy lapses.

RHIOs consist of many cooperating health care organizations and data sources, but the chain of trust in a RHIO is relatively short. The users from one organization are familiar with the other organizations within the community, so these are easier to organize than trust linkages on a larger scale.

In Washington, discussions are under way about how to expand these networks to a national scope and make them safe and secure. In another paper in this issue, McGraw and colleagues accept the use of health information exchanges for their stated purposes, but argue for additional

Director of Lister Hill National Center for Biomedical Communications- National Library of Medicine, Telephone - 301-496-4441, Fax - 301-435-3146, Address - 8600 Rockville Pike 38A 7N707, Bethesda, Maryland 20894, clemmcdonald@mail.nih.gov.

Conflicts- none

The opinions expressed here are those of the author and do not necessarily reflect the positions of the National Library of Medicine, the National Institutes of Health or the U.S. Department of Health & Human Services.

strictures because of the potential privacy risks at the national level. Others take this same position.

No one will disagree with the need for extra controls over access at the national level - or what is more commonly referred to as the Nationwide Health Infrastructure (NHIN). Indeed all current proposals for transfer of data at the national level include some additional constraints over the movement of data between RHIOs.

One strong control would be to allow the Patient (or his/her agent but no one else) to initiate a transfer of their RHIO data from where it resides to another RHIO. Under this model, the patient (or her agent) would log onto the RHIO or a care organization within the RHIO, pick a destination RHIO and ship a copy of their record to that RHIO. In the fall, Snowbirds could use this approach to copy their records to South Florida or Phoenix, and do vice versa in the spring. For emergency care, when outside of their home RHIO, patients (or their agents) could do the same when they reached the emergency room. In this model, government care systems like the Veterans Administration might define them as a one large RHIO or declare that their individual hospitals and clinics be part of the RHIO where they are located.

The requirement for patient control of cross-RHIO accesses will sometimes cause delays in acquiring clinical data from beyond the local RHIO. But most patient care is local. For example, among patients who were seen in Emergency rooms of a Midwest City, fewer than 2% visited any out of state pharmacy within the preceding year.² So such delays will have little effect on the overall care process.

This approach is simple and should be easy to implement, because similar data transfer systems such as that used by Google's Personal Health Record are already in operation. One could imagine variants of this model in which the patient could request continuous synchronization of their records within two or more RHIOs. This feature would accommodate people who lived on the border between two RHIOs and sought care from providers in both.

The specifics of my proposal to constrain data access at the national level are not important. What is important is that decision makers treat the control of access at the national level differently from control at the local (RHIO) level.

At the national level where the potential risks are high, and the data needs are low, we should add new barriers to access. At the local (RHIO and health care organization) level where the risks are low and the needs are high, we should not. To say it another way, policy makers should not add new constraints on access to RHIO data by clinicians, who are part of that RHIOs

McGraw and colleagues seem to recommend- because it would violate century old traditions, hinder innovation, discourage RHIO usage by clinicians, and discourage participation by health care organizations. Nor should policy makers re-shape the HIPAA privacy rule regulation as McGraw and also suggest without substantial justification

The Department of Health and Human Services (HHS) invested nearly six full years to create the HIPAA standards including the time required to dissect and understand the myriad issues, hold hearings, propose rules, review and respond to comments -- more than 50,000 of them and then write and polish the final rules. For years, the authors of the HIPAA regulation invested their days, nights and weekends on this mighty and heroic effort. Their final product is fifteen hundred dense pages long. And though it is a long and difficult read, it is a well thought out set of clear and decidable rules about the accepted use of protected health information. It is a good thing.

Now that the rule is finally working smoothly, it is time to praise HIPAA, not to bury it. HIPAA has produced what can only be called a revolution in sensitivity and attention to privacy issues in health care. Thus HHS deserves a chance to rest on its laurels and turn its attention to other pressing problems, such as the expected depletion of Medicare Part A's trust fund in 2019.

If there is a problem with HIPAA, the McGraw and colleagues complaints do not prove it. For example, their negative remarks about HIPAA's role in health information exchanges are: "it is not clear that health information exchanges have to enter into business associate agreements to exchange protected health information." But it *is* clear. Health data exchanges have business associates agreements (BAA) with the covered entities that provide them data. Thus they can perform any data task under HIPAA *on behalf* of the covered entity that the covered entity could perform itself. So exchanges *can* provide clinical data for treatment purpose to care providers without a business associate agreement because the covered entity can do so. I don't see that as a HIPAA flaw. How else could health data exchanges serve their clinical users otherwise?

Another criticism misses its mark altogether. McGraw and colleagues argue that HIPAA's de-identification is meaningless because it is too easy to re-identify such data. But the paper they cite to prove their point (reference 13) proves the opposite.³ The authors of that paper reported that they could re-identify their test data set when it included attributes such as birth date and full zip code, attributes that HIPAA forbids. However, at the end of the paper the same authors reported that they could *not* re-identify that data set when they followed the HIPAA rules and removed the forbidden attributes.

McGraw and colleagues also argue that HIPAA enforcement is not adequate because there have not been enough fines, but that begs the question. The Office of Civil Rights (OCR) received nearly 23,000 complaints in the first 29 months of HIPAA⁴. At least 2.5 billion medical visits occurred during that time period; so the complaint rate was 1/100,000 visits. As points of reference, complaints about the airline industry occurred at a rate of 9/100,000 boarding's in 2008; complaints about the care of institutionalized mental patients, at a rate of 9/100,000 residents⁵; and, in its first year, complaints about part D Medicare, at the whopping rate of 1800/100,000 Medicare patients⁶. These rates are not directly comparable, but the HIPAA rate of complaints is nominally low and if anything, it suggests HIPAA has succeeded wildly.

Further, the Office of Civil Rights (OCR) deemed that 72% of these 23,000 complaints were not worthy of pursuit, because they were not complaints at all or were not related to HIPAA privacy regulations, and, of those that OCR did pursue, it was able to induce corrective action in nearly 70% of them.⁷ Isn't that exactly what we want-- abiding changes in process and behavior? Or do we want retribution for its own sake.

Complicated rules and regulations have been around for literally thousands of years. And the fact that such rules can be numerous complicated and difficult to follow has been noted for as long. So before we rush to judgment about infractions of HIPAA and before we choose to make the rules even more complicated we should read the words that Ye Tian's wrote in 350 BC!

"When laws and commands are many, the people become uncertain about which [forbidden action] they should be avoiding." "The laws of Ch' in were as profuse as autumn tendrils and their network was as thick as congealed tallow... The officials cannot read them all, and all the less can the simple people do so. This is why law suits grow ever more numerous and why infractions committed by the people are ever more manifold. "Ye Tian lun" ⁸

References

1. McDonald CJ, Overhage JM, Barnes M, Schadow G, Blevins L, Dexter PR, Mamlin BW. The Indiana network for patient care: a working local health information infrastructure (LHII). *Health Affairs* Sept/Oct;2005 24(5):1214–1220. [PubMed: 16162565]
2. Simonaitis, Linas, MD; McDonald, Clement J, MD. Using National Drug Codes and Drug Knowledge Bases to Organize Prescription Records from Multiple Sources. *American Journal of Health-System Pharmacy*. 2009 accepted.
4. HIPAA Violations and enforcement. American Medical Association; 2008.
5. Hennessy K, Green-Hennessy S, Hijazi K. State Variations in Complaints Rates to Protection and Advocacy Systems. *May Psychiatr Serv* 2002;53:535.
6. United States Government Accountability Office. Report to Congressional Requesters “ Medicare Part D . Complaint Rates are Declining, but Operational and Oversight Challenges Remain. 2008. <http://www.gao.gov>
7. Martino, M. Less than 25% of Medical Privacy complaints Merit HHS Investigation . 2006 Dec 12. Available http://www.businesswire.com/portal/site/google/?ndmViewId=news_view&newsId=20061213005889&newsLang=en
8. Hsiao, KA. History of Chinese Political Thought. Mote, FW., translator. Princeton University Press; Princeton (NJ): 1979. p. 466