Health Privacy Is Difficult but Not Impossible in a Post-HIPAA Data-Driven World

Nicolas Terry, LLM

In the 13 years since their promulgation, the Health Insurance Portability and Accountability Act (HIPAA) rules and their enforcement have shown considerable evolution, as has the context within which they operate. Increasingly, it is the health information circulating outside the HIPAA-protected zone that is concerning: big data based on HIPAA data that have been acquired by public health agencies and then sold; medically inflected data collected from transactions or social media interactions; and the health data curated by patients, such as personal health records or data stored on smartphones. HIPAA does little here, suggesting that the future of health privacy may well be at the state level unless technology or federal legislation can catch up with state-of-the-art privacy regimes, such as the latest proposals from the European Commission.

ABBREVIATIONS: ACA = Affordable Care Act of 2010; EMR = electronic medical record; FTC = Federal Trade Commission; HHS = US Department of Health and Human Services; HIPAA = Health Insurance Portability and Accountability Act; HITECH = Health Information Technology for Economic and Clinical Health Act; OCR = Office for Civil Rights

Historically the dense Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules have been disliked almost as much by privacy advocates as they are by the providers they regulate. Yet the HIPAA rules of today are different in some important ways from those that struggled out of the US Department of Health and Human Services (HHS) bureaucracy in the last weeks of the Clinton administration. The domain within which they operate has changed even more. Health care and patient information are being reshaped not only by the Affordable Care Act of 2010 (ACA) but also by rapidly evolving research priorities, data markets, and online patient behaviors. Unfortunately, notwithstanding steady improvements to the core HIPAA model, changes in context now more than ever expose its limitations. This article reflects on changes to the HIPAA regime over the past 15 years and discusses the relationship of data protection with increasingly data-driven medicine. In particular, it flags the proliferation of health-related data and services that lie outside traditional health care and to which HIPAA does not apply, resulting in dramatically reduced patient protection that should be addressed with legislation that limits the collection of medical data.
An Improved HIPAA?
The original HIPAA privacy rule was tweaked almost as soon as it was published after incoming President George W. Bush ordered a rethink. One of the relatively minor changes made thereafter raised the ire of privacy advocates because it removed the symbolic privacy moment when a provider had to request the patient’s consent for data collection and processing (hardly a shocking requirement for an industry that had grown to live with, if not love, informed consent). The intervening years have witnessed more tweaks, but in the proprivacy direction, and the evolution of industry best practices to deal with the regulatory requirements of not only the privacy rule but also its companion security rule. However, all those changes paled before the changes introduced by the 2009 Health Information Technology for Economic and Clinical Health Act (HITECH).

HITECH did not attempt to cure the major flaws in HIPAA, such as the failure of HIPAA to control what patient information is collected and for what purposes or the generally unimpeded flow of data beyond the circle of care. However, it did limit some secondary uses of data by tightening up the consent processes for the marketing and sale of patient data. HITECH (and the various rule-making it authorized, eg, the 2013 Omnibus Rule) also reconfigured the legal relationship of business associates, such as a hospital’s outsourced services that require access to patient information. Business associates are now directly subject to the Privacy Rule and, more importantly, to its enforcement and penalties. HITECH also introduced a new model of data protection (or at least new to health care)—breach notification that requires health-care entities and their business associates to report when patient data are compromised. Serious breaches are publicized on the HHS “wall of shame” website. There is still more HITECH-authorized regulation in the pipeline, with accounting for disclosures likely being the most challenging for health-care entities.

Overall, it was in the realm of enforcement that HITECH brought about the greatest upgrade to HIPAA. The 2009 legislation introduced increased penalties, but arguably, the more important change was the Obama administration restructuring of enforcement under the Office for Civil Rights (OCR) and the appointment of an experienced prosecutor as its leader. OCR enforcement has become highly visible, investigating large privacy and security breach cases and levying headline-grabbing penalties (including one for $4.3 million).

Data-Driven Health Care
Although the HIPAA rules have evolved, the context in which they must operate has changed quite dramatically. The HIPAA 1996 Administrative Simplification (onto which was grafted regulatory authority for the privacy and security rules) was an attempt by health care to catch up with other industries in adopting e-commerce transactional models. In that context, the data challenge (and so the data protection challenge) was more about the business of health care (particularly communications between insurers and providers) than about its clinical aspects. The clinical data challenge arrived in 2009. As is well known, adoption of health information technology and, in particular, electronic medical records (EMRs) had been painfully slow, but HITECH, as part of the American Recovery and Reinvestment Act, included generous meaningful use subsidies for EMRs.

As clinical data have been pried from paper record silos, so have demands for data liquidity (access, sharing with patients, and interoperability between systems) escalated. HITECH also provided $1.1 billion in funding for comparative effectiveness research, spurring data-driven research (and inevitably demands for access to electronically stored clinical records). Such funding largesse would be repeated, albeit with more structure, with the ACA’s new programs for outcomes and patient-centered research. Increasingly, data are also the glue that holds together ACA’s next-generation care and financing models, such as Affordable Care Organizations and the Patient-Centered Medical Home.

New Sources of Medical Data
In parallel to the data-led transformation of the health-care system itself there is an increased demand for medical data outside traditional health care or the traditional health-care relationship. Unfortunately, some of this demand is being satisfied by criminal activity. Medical data theft has been steadily increasing, with the health-care sector becoming the leading target for cyberattacks in 2013.

The largest customers for legally acquired medical data are data brokers who sell business intelligence based on their processing of “big data.” These data brokers are collecting, storing, and analyzing petabytes of medical data. The sources of these data are extremely varied but include medically inflected data derived, for example, from social media trails or over-the-counter retail...


Although those outside traditional health care increasingly covet medical data, an increasingly large amount of medical data is originating from outside the traditional domain. Most intriguingly, patients are pursuing their own data strategies. Consumers are enthusiastically adopting mobile “app” and web technologies that implicate health data collection. These technologies include wellness and fitness products or health indicator trackers. Such technologies increasingly require or encourage personal data curation by patients themselves rather than by HIPAA-regulated providers.

All these rapidly changing contexts for the use and creation of medical data have serious implications for our understanding of privacy and security. HITECH itself is the poster child for the problems posed by data-driven health care; the same statute that delivered a significant upgrade to HIPAA also stimulated the adoption of EMRs designed to accelerate the widespread sharing of clinical data. However, it is likely that big health data services, mobile health apps, and patient data curation are the more serious developments because they directly undercut the HIPAA model of data protection.

HIPAA Limitations and Unprotected Data

This conclusion is likely because of three fundamental limitations in the HIPAA-HITECH construct. First, its data protection model operates downstream, regulating confidentiality, not privacy; that is, it only controls the dissemination of health data, not their collection. This counterintuitive description of our well-known privacy rule is valid because nowhere does HIPAA privacy impede, control, or regulate the collection of personal data. Logically, it would seem easier to protect (keep confidential) smaller amounts of data, but that was lost on the HIPAA architects and ignored by health-care stakeholders. Every discussion of secondary use or data breach can be traced back to this basic flaw: Failure to control data collection inevitability heightens disclosure problems.

Second, the HIPPA-HITECH model does not protect all health data. Rather, it only applies to certain forms of health data controlled by a limited group of data custodians. These covered entities are traditional, bricks-and-mortar providers, such as physicians, hospitals, pharmacies, health maintenance organizations, and health insurers. Thirteen years ago, that did not seem like a terrible policy decision. The storage and processing of petabytes of data were infeasible while the Internet and the World Wide Web were in their infancy and wearable computers and smartphones still seemed the stuff of science fiction. Today, however, vast amounts of medical data flow around in what may be termed “HIPAA-free space,” essentially unregulated. This is true of what was once HIPAA data that were acquired by public health agencies and then sold and medically inflected data collected from transactions or social media interactions. It is also true of much of the health data curated by patients themselves, including personal health records (eg, blue button downloads from the Veterans Administration and the Centers for Medicare & Medicaid Services) or health-related data stored on smartphones or personal computers.

Third, HIPAA created what lawyers call a liability rule. Such a rule imposes obligations on specific persons to refrain from particular conduct in a defined context. The classic example of a liability rule (and a HIPAA progenitor) is the duty of confidentiality derived from the physician-patient relationship, a relationship built on trust and respectful of patient autonomy. In that context, a patient would exercise his or her autonomy rights and divulge information to his or her physician. Because of the fiduciary nature of the relationship, the physician thereafter would hold the disclosed information in confidence and would be liable to the patient for unauthorized disclosures. This trust model does not scale well, and the simple bilateral physician-patient relationship on which it was based has all but disappeared in the face of more industrial, institution-based care models. Therefore, HIPAA identified a far broader cohort of providers (covered entities) who would be liable for unauthorized disclosures but vested the liability rights in a regulator (HHS) rather than in the patient.

This is not a particularly unsound rule when the data are being used by the same entity and for the same purpose for which it was collected. However, once data migrate to so-called secondary uses, a liability rule is far less effective from a patient perspective. This problem escalates outside HIPAA-protected space when the
A data subject may have no idea where his or her data originated but wishes to control its use. One legal alternative to a liability construct is a property rule. Such a rule is less interested in the original relationship, the context, or even good or bad conduct. Rather, it concentrates on the thing being protected. If we were to wrap health data with a property-like rule, privacy protection would attach to the data to the benefit of the data subject wherever the data ended up or in whomever’s hands.

Enduring State Health Privacy Laws

Some state health privacy laws do not share all the flaws of HIPAA. Of course, the very fact that any state privacy laws survive may be surprising. Although as a matter of law HIPAA did not replace (or preempt) state privacy laws that had more stringent privacy requirements, it seemed probable that state privacy laws would be crowded out by federal rules backed by better-funded enforcement.

It should be no surprise that California remains a protective outlier. Its original Confidentiality of Medical Information Act predated HIPAA, and its current code has a considerably broader reach than HIPAA. For example, the requirement that health data be kept confidential applies to health data custodians who are not traditional health-care providers, such as suppliers of personal health records services. In 2013, the obligation was amended to extend to software and hardware vendors of mobile health apps and devices. More recently, the state established an Office of Health Information Integrity to “ensure the enforcement of state law mandating the confidentiality of medical information and to impose administrative fines for the unauthorized use of medical information” and requiring all providers to “establish and implement appropriate administrative, technical, and physical safeguards to protect the privacy of a patient’s medical information.”

Perhaps more surprising is the new Texas legislation. Whereas HIPAA applies to a relatively narrow group of covered entities, the Texas statute applies to “any person who…engages…in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information.” The same statute also requires “clear and unambiguous permission” before health information may be used for marketing and broadly prohibits the sale of an individual’s protected health information.

Another area where state law has shown robustness is in private rights of action. As is well known, HIPAA does not permit injured individuals to bring an action for breach of the privacy or security rules. However, state common law torts (and even some state statutes) permit such actions, leading to a steady stream of primarily data-breach cases being filed in state courts. For example, a case of a stolen laptop applying Florida law took a position generous to the plaintiffs in showing a causal relationship between a data breach and alleged identity theft.

Privacy advocates likely applaud such state law positions as both real improvements to data protection and interesting “states as laboratories” examples for possible future federal adoption. On the other hand, providers, particularly those who operate across state lines, likely decry the additional indeterminacies and other costs strewn in their path.

Rethinking Health Privacy

Regulatory enforcement will always somewhat depend on the vagaries of the political process and budgeted resources. Notwithstanding, it is likely that today’s evolved HIPAA will continue to be a reasonably strong model, albeit one that does not control data collection but does a decent job restricting unauthorized access or disclosure held by health-care providers. Increasingly, however, it is not the medical data contained within the traditional health-care system that will be of primary concern; rather, it is the health information circulating in the HIPAA-free zone that is concerning. Here, true privacy controls that limit the collection and retention of data are required. At the very least, the use or processing of medical data or medically inflected data should be restricted to the purposes for which such data were originally collected.

In 2012, both the White House and the Federal Trade Commission (FTC) published proposals along these lines. With a little effort, these privacy proposals could have been reworked to complement the confidentiality model of HIPAA. However, since the election, the White House seems to have lost interest in a privacy legislative agenda, although at a broad policy level, it has exhibited some recent interest in big data issues. Interestingly, the FTC is also showing increased interest in medical data. In a recent ruling dealing with a clinical testing laboratory and allegations of “unfair...acts or practices,” the commission rejected the argument that HIPAA or HITECH prevented it from exercising its general powers. At least one implication is that the FTC is interested in protecting medical data in general
rather than viewing them as the exclusive domain of the HHS OCR.

Meanwhile, the body most influential in privacy matters is once again leaping ahead. The European Commission is building on its landmark data directive with a draft regulation that adds a renewed commitment to proportional data collection, limitations on data profiling, breach notification, and streamlined enforcement. The proposed legislation also includes the type of property rule discussed in this article, giving the data subject rights that run with the data, including a right of data erasure (ie, the right to be forgotten).28

Health privacy is complex. As with so many other medicolegal issues, the answers have become increasingly difficult as health care has gone through its various structural and funding metamorphoses. When the traditional bilateral physician-patient relationship was dominant, it could temper the amount of information collected by the physician and reasonably calibrate the parties’ expectations about future disclosures. Separated from that relationship, the processes and answers are less obvious. Patient relationships with multiple physicians and institutional providers resist most nuanced or personalized constructs dealing with data. In their stead, instrumentalism tends to dominate, favoring maximum initial disclosure and, thereafter, relatively unlimited data sharing. This tendency is amplified by the increasingly public good approach to patient data desired for health-care and other research.29 As we embrace population health and repurpose aggregated patient data to drive public health, clinical, outcomes, and comparative effectiveness research, the privacy interests of individual patients often are viewed as barriers. Patients deserve to have their medical data protected far more effectively, whether circulating inside or outside traditional health-care spaces.

Acknowledgments

Financial/nonfinancial disclosures: The author has reported to CHEST that no potential conflicts of interest exist with any companies/organizations whose products or services may be discussed in this article.

References

15. See, for example, Hawaii Health Care Privacy Harmonization Act 2012, which reduced state protections to the federal norm.
17. Cal Health and Safety Code §130203(a)
18. Tex Health & Safety Code Ann §181.001(b)(2)
19. See, for example, Acara v Banks, 470 F3d 569, 572 (5th Cir 2006).