Moving Toward a New Health Care Privacy Paradigm

By Kirk J. Nahra

November 2014

The Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA) has set the primary standard for the privacy of health care information in the United States since the rule went into effect in 2003. It is an important rule that creates significant baseline protections for health care information across the country.

Yet, from the beginning, the HIPAA Privacy Rule has had important gaps. The Privacy Rule was the result of a series of Congressional judgments about "scope"—driven by issues having nothing to do with privacy, like the "portability" of health insurance coverage and the transmission of standardized electronic transactions. As a result of the HIPAA statute, the U.S. Department of Health and Human Services (HHS) only had the authority to write a privacy rule focused on HIPAA "covered entities," meaning that certain segments of relevant industries that regularly use or create health care information—such as life insurers or workers compensation carriers—were not within the reach of the HIPAA rules. Therefore, the HIPAA Privacy Rule has always been a "limited scope" privacy rule, rather than a general medical privacy rule.

But, at least at the start, these gaps were somewhat limited, and large components of the health care industry—including most health care providers and health insurers—were covered by the HIPAA. What has changed in the past decade is the enormous range of entities that create, use and disclose health care information outside of the HIPAA privacy rule. We have reached (and passed) a tipping point on this issue, such that there is enormous concern about how this "non-HIPAA" health care data is being addressed, and how the privacy interests of individuals are being protected (if at all) for this "non-HIPAA" health care data.

So, what exactly is the problem and what is likely to happen to address it?

We have seen in recent years an explosion in the creation of "non-HIPAA" health care data. For example, numerous web sites gather and distribute health care information without the involvement of a covered entity (meaning that these web sites are not covered by the HIPAA Privacy Rule).

* * *

Kirk J. Nahra is a Partner with Wiley Rein LLP in Washington, D.C. He represents a wide variety of companies on privacy, data security, cyber-security, and security breach issues across the country and internationally. He chairs the firm's Privacy and Data Security practice. A long-time member of the Board of Directors of the International Association of Privacy Professionals and editor of IAPP's Privacy Advisor, he speaks and writes widely on a broad variety of privacy and data security issues. He can be reached at 202.719.7335 or knahra@wileyrein.com. Follow him on Twitter @kirkjnahrawork.

These range from commercial web sites (e.g., Web MD), to patient support groups, to the growth of personal health records. We also have seen a significant expansion of mobile applications directed to health care data or offered in connection with health information. Recent announcements from Apple and Google have expanded this large and growing area. Unless a covered entity is involved, these activities generally are outside of the scope of the HIPAA Privacy Rule, and are subject to few explicit privacy requirements (other than general principles such as the idea that you must follow what you say in a privacy notice).

This growth in "non-HIPAA" health care data is raising significant expressions of concern, by the FTC, privacy advocates and others, about how (if at all) this "non-HIPAA" health data is regulated and how the privacy interests of consumers are protected. As FTC Commissioner Julie Brill stated in a recent speech, "Big picture, consumer generated health information is proliferating, not just on the web but also through connected devices and the internet of things." As Ms. Brill indicated, this development involves "health data flows that are occurring outside of HIPAA and outside of any medical context, and therefore outside of any regulatory regime that focuses specifically on health information."

At the same time, we also have seen increasing discussion of the general concept of "Big Data" and the impact of "Big Data" on privacy and security.

While much of this discussion is outside of the context of health care, there is both a wide variety of health care information (HIPAA regulated and not) that is being scrutinized in the context of Big Data and a growing range of "Big Data" activities being conducted by health care entities, again both in and out of HIPAA.

In the context of this development, a recent White House report on Big Data stated that:

- A significant finding of this report is that big data analytics have the potential to eclipse longstanding civil rights protections in how personal information is used in housing, credit, employment, health, education, and the marketplace.

- The privacy frameworks that currently cover information now used in health may not be well suited to address these developments or facilitate the research that drives them.

- As big data enables ever more powerful discoveries, it will be important to re-visit how privacy is protected as information circulates among all the partners involved in care. Health care leaders have voiced the need for a broader trust framework to grant all health information, regardless of its source, some level of privacy protection.

- This may potentially involve crafting additional protections beyond those afforded in the Health Insurance Portability and Accountability Act and Genetic Information Non-Discrimination Act as well as streamlining data interoperability and compliance requirements.

Modernizing the health care data privacy framework will require careful negotiation between the many parties involved in delivering health care and insurance to Americans, but the potential economic and health benefits make it well worth the effort.

These developments have identified several significant concerns that are motivating this debate. First, much of the data that is being gathered is outside the scope of the HIPAA rules (and is therefore largely unregulated). The volume of this data is growing. Accordingly, there is a key issue as to how, if at all, this "non-HIPAA data" should be regulated.

Next, through the White House Big Data report, the FTC's Data Broker report and otherwise, substantial concerns have been raised about how this data is being used, in contexts that raise questions about how health care services are provided and appropriate rights and protections for individuals in connection with their health care and their privacy.

In addition, as "patient engagement" becomes an important theme of health care reform, there is increased concern about how patients view this use of data, and whether there are meaningful ways for patients to understand how their data is being used. The complexity of the regulatory structure (where protections depend on sources of data rather than "kind" of data), and the difficulty of determining data sources (which are often difficult, if not impossible, to determine), has led to an increased call for broader but simplified regulation of health care data overall. This likely will call into question the lines that were drawn by the HIPAA statute, and easily could lead to a re-evaluation of the overall HIPAA framework. In fact, this issue was raised specifically by Commissioner Brill in her recent speech, where she asked:

> then the question becomes, though, if we do have a law that protects health information but only in certain contexts, and then the same type of information or something very close to it is flowing outside of those silos that were created a long time ago, what does that mean? Are we comfortable with it? And should we be breaking down the legal silos to better protect that same health information when it is generated elsewhere.

At the same time, we also are seeing an increased usage by HIPAA covered entities of personal data that would not traditionally be viewed as "health care information." For example, a recent report published on Bloomberg.com discussed how physicians are obtaining a wide variety of behavioral indicators about their patients in order to monitor health risks. The story states that "You may soon get a call from your doctor if you've let your gym membership lapse, made a habit of picking up candy bars at the check-out counter or begin shopping at plus-sized stores." See Pettypiece and Robertson, "Your Doctor Knows You're Killing Yourself. The Data Brokers Told Her," (Bloomberg.com, June 26, 2014), available at http://www.bloomberg.com/news/2014-06-26/hospitals-soon-see-donuts-to-cigarette-charges-for-health.html. Similarly, the New York Times reported on "health plan prediction models" that use consumer data obtained from data brokers, such as income, marital status, and number of cars owned, to predict emergency room use and urgent care needs. See Singer, "When a Health Plan Knows How You Shop," (New York Times June 28, 2014), available at http://www.nytimes.com/2014/06/29/technology/when-a-health-plan-knows-how-you-shop.html?_r=0. This kind of information usage by HIPAA covered entities—relying on data

that is not traditionally viewed as health care information and which is widely available outside of health care contexts and for a wide variety of non-health care usages—threatens to blow up the concept of what "health information" means.

This convergence of data creation and usage is leading to an increasing debate about what should be done—if anything—about this "non-HIPAA" health care data and the application of HIPAA Privacy Rules to data that does not directly involve the provision of health care. It is clear that this debate will be ongoing and extensive. It is not clear at all what the results of the debate will be.

Therefore, companies in virtually all industries—those in the health care industry, those that create, gather, and use any kind of health care data and those companies that create and disclose data that might be used for some kind of health care purpose—all need to evaluate how this debate affects them and what their role will be in the debate (and how their behavior might need to change in the future).

Each company should think about the following questions.

First, *how might this debate proceed?*

At a minimum, there are several options. Moving from "most limited" to "broadest" in application, we could see specific proposals approaching this issue in the following ways:

- A specific set of principles applicable only to "non-HIPAA health care data" (with an obvious ambiguity about what "health care data" would mean);

- A set of principles (through an amendment to the scope of HIPAA or otherwise) that would apply to all health care data; or

- A broader general privacy law that would apply to all personal data (with or without a carve-out for data currently covered by the HIPAA rules).

The first option would address this specific problem of the generally unregulated nature of non-HIPAA health care data. The second approach would create a uniform set of standards for all health care data. The last—and clearly broadest—option would recognize the difficulty in drawing the line on what is "health care data" and would create a broad set of principles for all personal data.

With these three general approaches in mind (and recognizing that each of these can have material variations), *each company should think about how this debate (and any resulting rules) would apply to you.* Are you currently covered by the HIPAA rules, as a covered entity or business associate? Do you obtain or create health care information that is either in or out of the HIPAA structure? Do you participate in business activities involving health care data that are outside the scope of HIPAA? Would a "HIPAA-like" regulation for these "non-HIPAA" activities help or hurt your business? Are you at a competitive advantage or disadvantage because of this existing set of rules?

Last, with these impacts in mind, what should your company's role be in this debate? Would a new set of rules about this "non-HIPAA" data help or hurt your business? What do you want the outcome of this debate to be?

If there are rules for this non-HIPAA data, would you like them to be the same or different from the HIPAA principles? Would you like these rules applied more broadly to all personal data? Or is there a reasonable basis for a preference to regulate only health care data?

Conclusions

While the ultimate outcome of this debate is unclear (and may remain unclear and under debate for an extended period of time), it is clear that concerns about "non-HIPAA" health care data are not going away. There simply is too much interest in "doing something" about these issues for the discussion to stop. The debate will move forward, affected groups will make proposals, regulators will opine, and legislative hearings will be held. Industry groups may choose to develop guidelines or industry standards to forestall federal legislation. At a minimum, the policy-making "noise" on this issue should be substantial and ongoing for at least the next several years. It is clear that we are a long way from any agreement or consensus on defining any new rules to address these concerns, despite the growing consensus that there is a need to do something on these issues.

The challenge for your company is to understand these issues and how they could affect you, and to think carefully and strategically about your role in the debate and how these issues will affect your business going forward.

* * *