The Pandemic and the Ongoing Evolution of Health Care Privacy

By Kirk J. Nahra[1]

I have been involved in the evolution of privacy law since the topic started to become a significant issue for American companies in the very late 1990s. I am a practicing attorney in Washington, D.C at WilmerHale, where I co-chair the firm's global Cybersecurity and Privacy Practice. I also teach privacy law, at the Washington College of Law at American University as well as guest teaching at other schools, including Washington University in St. Louis. I am honored to serve as a fellow with the Cordell Institute for Policy in Medicine & Law at Washington University. My biggest focus of attention has been on privacy issues involving the health care industry and health data. So my perspective on these issues covers compliance, practical business needs and the more theoretical aspects of privacy law.

When I teach privacy law, I try to make the issues real for the students. It often isn't that hard — privacy issues remain in the news almost every day. I also believe that the challenges and issues facing the health care industry are among the most complicated and interesting in all of privacy law– because of the wide variety of interested stakeholders involved in any discussion of health care privacy. When you go to a store to buy jeans, or visit a web site, there are interests of the company you are dealing with and your personal privacy interests. But that's pretty much about it. For health care, we have to think about the average patient, the patient with a significant or sensitive condition, employers, government as regulator, health care provider and payer, the health care industry in general, taxpayers, medical research and a variety of other interests. These make privacy debates particularly challenging in the health care industry. You can't think thoughtfully about privacy law issues without considering health care, and you can't think effectively about health care without considering privacy.

The evolution of the pandemic has made more of these issues real and is leading to a series of critical questions for the future of health care privacy that are evolving in real time. These issues are not new, but the focus of the attention on pandemic issues has made the need for discussion and resolution of these issues even more critical.

HIPAA Background

To understand how the pandemic is affecting health care privacy, it is critical to understand the context for health care privacy today. The Privacy Rule stemming from the Health Insurance Portability and accountability act of 1996 ("HIPAA") has set the standard for the privacy of health care information in the U.S. since the rule went into effect in 2003. This is the major national standard for health care privacy in the United States today.

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" and driven by issues having nothing to do with privacy, like the "portability" of health insurance coverage and the

[1] Kirk J. Nahra is a Partner with WilmerHale in Washington, D.C., where he co-chairs their global Cybersecurity and Privacy Practice. He is a Fellow with the Cordell Institute for Policy in Medicine & Law at Washington University in St. Louis. He also teaches privacy law at the Washington College of Law at American University.. He can be reached at 202.663.6128 or kirk.nahra@wilmerhale.com. Follow him on Twitter @kirkjnahrawork.

transmission of standardized electronic transactions. As a result of the HIPAA statute, the Department of Health and Human Services only had the authority to write a privacy rule focused on HIPAA "covered entities" (health care providers, health plans and health care clearinghouses). This meant that, from the start, certain segments of relevant industries that regularly use or create health care information were not within the reach of the HIPAA rules. Therefore, the HIPAA Privacy Rule has always been a "limited scope" privacy rule. Bound by the statutory framework, the Privacy Rule focuses on "who" had your health care information rather than the information itself.

While these gaps existed from the beginning, most components of the traditional health care industry were covered by the HIPAA rules. What has changed in recent years is the enormous range of entities that create, use and disclose health care information outside of the reach of the HIPAA rules. 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.

Because of the limited scope of the HIPAA statute, a broad range of entities that collect, analyze and disclose personal health information are not regulated by the HIPAA rules. For example, numerous websites gather and distribute health care information without the involvement of a covered entity (meaning that these websites are not covered by the HIPAA Privacy Rule). We have seen a significant expansion of mobile applications directed to health care data or offered in connection with health information or overall wellness. The entire concept of "wearables" post-dates the HIPAA rules and generally fall outside the scope of HIPAA. Unless a HIPAA-covered entity is involved, these activities are generally outside of the scope of the HIPAA Privacy Rule and 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).

In addition, as "patient engagement" becomes an important theme of health care reform, there is increased concern about how patients view such uses 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 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. We see meaningful situations across the health care spectrum that involve data protected by HIPAA at one point and then, through permitted disclosures, no longer receives the protections of the HIPAA rules. These growing gaps call into question the lines that were drawn by the HIPAA statute and easily could lead to a reevaluation of the overall HIPAA framework.

The debate about whether and how to address these gaps has been in progress for many years. We saw a variety of thoughtful papers from the Federal Trade Commission, the Department of Health and Human Services and the Obama White House in the 2012-2016 period, addressing both these gaps in coverage and various potential risks associated with "big data" in this unregulated environment. We also have seen efforts to assess whether to extend the operation of the HIPAA Privacy Rule in connection with coordinated care, value-based care and emerging concepts related to social determinants of health. Some in Congress and elsewhere even blamed the HIPAA Privacy Rule for at least part of the opioid crisis.

Accordingly, there has been extensive discussion about the current health care privacy structure, where it works and where it doesn't, and how (if at all) it could be changed to fit today's health care environment. At the same time, over the past several years, the effort to look at these health care privacy issues on their own has largely disappeared, and has recently been subsumed by the questions about a national privacy law. One key policy question that is emerging is whether the complicated balances of health care privacy can effectively be addressed in a more general overall privacy law.

The Pandemic and Health Care Privacy

In this context, we are seeing four distinct categories of issues arising from the pandemic. These topics are not new, but the pandemic is both highlighting them and pushing the complicated policy challenges to the forefront.

- The differing interests of patients

We have seen over the past several years a variety of health care policy goals where there is a tension between an individual's interest in privacy and their interests in some other aspect of the operation of the health care system.

For example, in the recent federal debate over "information blocking," there was a substantial and visible (and mostly pre-pandemic) discussion about whether the interest of patients in having access to their medical information should take precedence over the protection of those records under the U.S. Health Insurance Portability and Accountability Act Privacy and Security rules. A variety of relevant stakeholders tried to find a "win-win" in this situation, but the eventual result is that — because of the limited scope of the HIPAA rules — there will be situations in which a patient's interest in receiving access to their medical records will mean that those records, once released, will not be subject to the full protections of the HIPAA Privacy and Security rules.

The primary choice in this situation was to favor a patient's interest in access to their records over their privacy and security interests (although the regulations tried to balance these the best they could).

A similar issue has played out with the recent Department of Health and Human Services enforcement guidance related to telehealth. As part of its pandemic response, HHS has made clear that it will not be taking enforcement action involving telehealth visits; this means that health care providers interested in providing telehealth services did not need to be concerned about the details of the HIPAA Security Rule in conducting these visits. Whether this enforcement waiver was required is a different question, but the clear intent is to provide support for telehealth visits at a time when telehealth visits are critical to the interests of patients in receiving health care.

Through this health care enforcement waiver, the government selected the benefits to consumers (and the health care system) from enhanced telehealth opportunities over the more specific privacy and security interest of the HIPAA rules.

- Balance between privacy interests and health care system interests

HHS also has issued other HIPAA guidance stemming from the pandemic. While the justification for these actions is less clear, the goal is to facilitate the operation of the health care system at a time when the system is stressed, by reducing otherwise applicable HIPAA obligations.

This has led to a waiver of certain HIPAA requirements (including the obligation to provide a privacy notice and an opportunity for a request for restrictions or confidential communication). This was a policy choice, but why this choice actually helped the system — at a clear detriment to privacy interests — is less clear.

Similarly, HHS has announced that business associates now can make disclosures of patient information for public health purposes – increasing the sources of public health disclosures is what the Privacy Rule previously seems to have permitted.

- How to address non-HIPAA health data issues (e.g., employee health data)

We also are seeing a focus on health care privacy interests during the pandemic where HIPAA is largely irrelevant. This is not a new issue. I have been writing about this issue of "non-HIPAA health data" for almost 10 years.

Here, however, the focus has been on health care information of employees and others in connection with access to business locations and business activities. This employee information is not subject to HIPAA (primarily HIPAA for most employers applies only through their health insurance benefits plan), but other laws, such as the Americans with Disabilities Act, clearly apply.

For site visitors, guests, service workers and others, there may be no generally applicable privacy law — at least in the United States — regulating how personal health information can be collected and used. This means that when companies in the U.S. think about how they can share specific health information about specific individuals, the current primary health care privacy law is irrelevant.

- How to address non-health data relevant to the health care system (e.g., location data for health monitoring)

Last, we also are seeing the evolution of a related health care issue: the increasing recognition in a variety of circumstances that information that isn't clearly about health does, in fact, matter when operating the health care system.

In the pre-pandemic HIPAA context, there was a regulatory proceeding where HHS was exploring whether to modify the HIPAA rules to permit, for example, the sharing of protected health information with social service organizations — even though these organizations do not fit cleanly into the HIPAA framework.

The inquiry reflects a recognition that social issues — food or housing needs, for example — can play an important role in the overall health of an individual. In the pandemic situation, we are focused now on location data and how it can be used for public health purposes. This data doesn't — by itself — say anything about your health, but it will be used to identify the

movements of individuals affected by the coronavirus and identify others for whom there also are health-related risks.

This is both a health care privacy and a civil liberties issue. It is exactly the kind of issue that is addressed throughout the HIPAA rules, where the smooth operation of the health care system was incorporated as a means of modifying otherwise applicable privacy interests.

But this is a different order of magnitude and one in which the full attention of society is focused on these issues in a way that HIPAA seldom catches the public's attention.

Concluding Thoughts

I raise these issues not because there is a clear or obvious answer. These clearly are difficult times, and we must take advantage of the opportunity presented by these pandemic challenges to evaluate the issues, but we must also be careful not to let the emergency circumstances dictate bad choices.

In the national privacy law debate, the role of the health care system has taken a back seat to the larger privacy debate. This is both understandable and problematic. The health care industry has viewed privacy law as relatively settled for many years, but we are increasingly recognizing that this is not really the case.

The HIPAA rules often work well where they apply, but there are both more situations in which they don't apply, and a broader range of events where the rules may not work well. The pandemic has led to the immediate need to address some of these complications in real time, but we will need to ensure that these issues remain in the public debate and that the increasing complexities of health care privacy can be addressed appropriately in any future U.S. privacy law.