The pandemic and the evolution of health care privacy

By Kirk Nahra

IAPP (May 6, 2020) -- 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. 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. 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.

We are seeing four distinct categories of issues arising from the pandemic.

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.

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.

Kirk J. Nahra is a partner with WilmerHale in Washington, D.C., where he represents companies in a broad range of industries in connection with privacy and data security laws and regulations across the United States and globally. He is co-chair of the firm's Cybersecurity and Privacy Practice. He is a nationally recognized expert on privacy and data security laws related to the health care and insurance industries. He assists companies in a wide range of industries in analyzing and implementing the requirements of privacy and security laws across the country and internationally, and provides advise on data breaches, enforcement actions, contract negotiations, business strategy, research and de-identification issues and privacy, data security and cybersecurity compliance. A graduate of Georgetown University and Harvard Law School, he teaches privacy law at the Washington College of Law at American University and is a Fellow with the Joseph and Yvonne Cordell Institute for Policy in Medicine & Law at Washington University and the Institute for Critical Infrastructure

Technology. He can be reached at 202.663.6128 or kirk.nahra@wilmerhale.com. Follow him on Twitter @kirkjnahrawork.