INSIGHT: The Top Five Health Care Privacy Issues to Watch in 2020

Published in Bloomberg Law (November 29, 2019) by Kirk Nahra –

WilmerHale's Kirk J. Nahra looks at the top five health care privacy issues for 2020. The HIPAA Request for Information takes center stage as the HHS looks for input on expansion of disclosures for value-based care, coordinated care, and to address the opioid crisis. Other things to watch include access rights and enforcement, the CCPA, and medical research privacy issues.

Kirk Nahra

The health care industry has had privacy and security rules since the early 2000s. These rules, stemming from the Health Insurance Portability and Accountability Act, provide some of the most important, comprehensive and evolved privacy rules in the country.

At the same time, it is increasingly clear that the HIPAA rules (1) do not apply to significant percentages of the health information that is created in the country; and (2) there are increasing complexities for a broad variety of health care stakeholders (including patients) because of this limited scope of the HIPAA rules.

These tensions are driving the focus of attention in 2020 for the health care industry and the broader range of entities that use, collect and analyze health care information.

The HIPAA RFI

For direct purposes of HIPAA, the big issue to watch in 2020 is the results—if any—of the broad Request for Information (RFI) issued by the Department of Health and Human Services (HHS). This RFI sought input on various issues related to the expansion of disclosures for value-based care, coordinated care, and to address the opioid crisis.

While OCR seemed to have a vision of potential problems from HIPAA, it did not provide obvious solutions to those problems—or any clear indication of what the problems actually were. This RFI may lead to nothing—many of the comments focused on a lack of problems on these topics and an acknowledgment that, to the extent any privacy laws were creating impediments in these areas, those were primarily state laws and Part 2 rather than HIPAA.

But we may see some new or broadened expectation of disclosures for these purposes. And remember, the RFI also addressed the long-delayed accounting rule changes—with no clear direction of any kind on this highly problematic provision.

Access Rights and Enforcement

We are always watching developments with HIPAA enforcement. For the most part, other than some waxing and waning of volume (and some very recent indications of expanded activity), enforcement proceeds along apace. Most cases have related to security problems, typically involving a failure to conduct an effective risk assessment. The HHS has new guidance on this topic.

The area I will be watching in 2020 is whether the HHS makes a meaningful change in its enforcement of HIPAA access rights. There are clear indications—from a highly publicized Ciitizen study and otherwise—that access is an ongoing problem. At the same time, there is a sense in the regulated community that access violations are small potatoes.

We will be watching whether the HHS makes a change in this area to focus more direct pressure on covered entities to ensure that this important individual right is protected effectively.

Non-HIPAA Health Data

The broader concern we are watching in 2020 involves the continued growth of "non-HIPAA" health care information. Because of the limited scope of the HIPAA rules, we are seeing a dramatically increased development of health related information that is being created, gathered and collected outside of the scope of the HIPAA rules, from mobile applications, wearables, patient support web sites, personal health records and the like.

This information is not exempt from privacy requirements, but generally is not subject to HIPAA. There had been efforts to evaluate the policy issues involving this data in prior years, but this effort largely has been swallowed up by the national debate on privacy legislation (with the noticeable exception of the Klobuchar-Murkowski bill (S.1842) that addresses this issue in isolation).

CCPA and the Health Care Industry

Part of this "non-HIPAA" issue is being addressed by the California Consumer Privacy Act. CCPA is creating problems across the entire privacy landscape, for companies in virtually every industry.

For the health care industry, CCPA creates three buckets of regulation—HIPAA (where covered entities largely are carved out from CCPA), entities regulated by the California Confidentiality of Medical Information Act (which applies to certain technology companies that are not regulated by HIPAA), and then CCPA for everyone else.

A consequence of this approach is that the regulatory approach for healthcare data will become even more fragmented, and consumers will have even less ability to understand the rules that apply to their health information, which will vary significantly based on specific details of the regulated entity.

At the same time we are seeing important elements of health care reform, where a more holistic approach to patient care that includes not only traditional health factors but also a broad variety of newer concepts loosely categorized as social determinants of health, creates real complications in the existing privacy structure.

The health care industry may need to evaluate whether it can stomach a "new" HIPAA that covers all this information.

Medical Research

Last, privacy also continues to create complications for medical research. In the U.S., the question of whether HIPAA impedes medical research has been pending since the rules went into effect in 2003. There is meaningful debate on this issue (although my personal view is that the rules are fine but understanding of them is not very strong).

At the same time, movement towards more personalized medicine is making it harder and harder to find appropriate patients for particular kinds of research and the potential benefits of secondary research on data without any direct patient impact are growing.

Also, there are real concerns about the privacy rules in Europe. There are new and current tensions between research and privacy rules, such that the industry does not currently understand how best to approach patient consent for research. In addition, different authorities in different countries (all operating under the single EU-wide GDPR) have come to different conclusions on the relationships between research sponsors and clinical trial sites—creating meaningful confusion and actual impediments to research.

Conclusion

The health care industry has generally been reasonably settled on privacy rules for many years. We are seeing today, however, a broad range of developments that may be creating real pressure to change the status quo, for the potential benefit of both consumers and the industry.

This column does not necessarily reflect the opinion of The Bureau of National Affairs, Inc. or its owners.

Author Information

Kirk J. Nahra is a partner with WilmerHale in Washington, D.C., where he co-chairs the global Cybersecurity and Privacy Practice. He represents companies in a wide range of industries in analyzing and implementing the requirements of privacy and security laws across the country and internationally, including advice on data breaches, enforcement actions, big data issues, contract negotiations, business strategy and overall privacy, data security and cybersecurity compliance.