Top Five Health-Care Privacy, Security Developments to Watch in 2021

Published in Bloomberg Law (December 9, 2020) by Kirk Nahra –

Health-care privacy is at a crossroads. For almost 20 years, the health-care industry has addressed the requirements of the HIPAA Privacy and Security Rules, building reasonable and appropriate compliance programs from an uncertain and awkward beginning.

The stability has been important, and the important choices made in the HIPAA rules to both protect individual privacy and allow the health-care system to work effectively generally have been a positive for consumers and the industry. But there always have been gaps in HIPAA's scope, and they are becoming more significant.


Kirk Nahra

New laws are imposing inconsistent obligations across different segments of the industry, and new elements of thinking about what "health care" is that are threatening the current structure. Next year may be a watershed year, with both health-care privacy as an independent variable, and potentially in connection with a national privacy law. Here's what to watch for in 2021.

1. HIPAA Notice of Proposed Rulemaking

The current HHS Office for Civil Rights disseminated a request for information related to the HIPAA Privacy Rule. It explored a variety of key issues involving use and disclosure of protected health information under HIPAA, generally focusing on expanded information sharing due to social determinants of health, concerns about the opioid crisis, and more.

The overall gist of the inquiry focused on mandating or encouraging more disclosures that are now permissive and exploring ways to share information outside the HIPAA system. It was clear that they had questions but not yet answers. A notice of proposed rulemaking is in the final stages and should be released before the new administration enters office.

2. Social Determinants of Health

The concept of social determinants of health is broadly entering the overall health-care discussion.

We now recognize that "non-health" factors such as overall nutrition and appropriate housing play important roles in an individual's health care. These factors have disproportionately impacted underserved and disadvantaged communities. The Covid-19 crisis has accentuated many of these gaps.

From a health privacy perspective, however, the HIPAA rules do not appropriately address these health-related implications outside of the traditional health-care system; we don't think of food banks and housing agencies as health-care providers. We can expect significant attention to these issues, with state Medicaid agencies leading the way.

3. Non-HIPAA Data and State Activity

The social determinants of health issues have also accentuated the longstanding issue of "non-HIPAA" health data. The HIPAA rules work well where they apply, but due to the contorted history of the HIPAA statute, much of the health-care information being created in our internet-connected era is outside of the reach of the HIPAA rules—from wearables, mobile health applications, community and patient support sites, and personal health records.

There had been some effort at the federal level to address these issues, but this progress was halted entirely over the past four years. It has now been enveloped in the overall national privacy debate. We are seeing states jump in from an enforcement perspective—with the New York and California attorneys general using enforcement to create new standards for this non-HIPAA health data. That is something for health companies

to watch but is not a long-term policy strategy.

4. The New Administration

While privacy has not been at the forefront of the new administration's attention, we will expect a broad variety of impacts from the change. We can expect entirely new management at the HHS Office for Civil Rights, with likely additional focus on HIPAA enforcement. We can expect the Federal Trade Commission to continue to review certain aspects of non-HIPAA health data.

We also should expect policymakers to restart the efforts from the Obama White House to review the impact of artificial intelligence and big data analytics in health care and the impact on disadvantaged communities.

5. The California Conundrum

While the national debate about a national privacy law putters along, we have enormous changes in California. Due to the California Consumer Privacy Act, if you are a California resident, your health information can be governed by at least six regulatory structures: (1) HIPAA itself (exempted from CCPA); (2) the Confidentiality of Medical Information Act, an odd HIPAA-like state law that also exempts its covered entities from CCPA; (3) clinical research (exempt from CCPA);(4) CCPA itself (which you might hope would apply to everything else); but (5) CCPA does not cover nonprofits and (6) CCPA does not cover employee data (including Covid-19 data collected by employers).

My view is that this approach is bad for both consumers and businesses, the rare privacy "lose-lose." While other states will not replicate this chaos, we can expect the California situation to put pressure on thinking about how health-care privacy should be addressed in a national privacy law (or in other state privacy laws).

'Hands-Off' Approach to Legislation May End

The health-care industry has been reasonably happy with the HIPAA structure, and has taken a "hands off" approach to new legislation at the state and federal levels. This position may become increasingly untenable.

As states and perhaps a national law address a wide range of health data, it will be important for both health-care consumers and the health-care industry to think carefully about how to address the broad range of health-care data, from all sources; the enormous amount of "non-health" information that increasingly is being used in the health-care system; and to address the need for what HIPAA to date has done.
That is, to appropriately balance meaningful privacy protection with the effective and efficient operation of the health-care system. This is a meaningful challenge and there's a long way to go.

This column does not necessarily reflect the opinion of The Bureau of National Affairs, Inc. or its owners.
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, including advice on data breaches, enforcement actions, big data issues, contract negotiations, business strategy and overall privacy, data security, and cybersecurity compliance.