COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 30, Number 14. April 12, 2021 Entities Deal With More Data Outside HIPAA; 'We Are Seeing Tensions'

By Nina Youngstrom

When employees are required to show their employers proof of a positive COVID-19 test before they get sick leave or a vaccination before returning to work, the implications are profound—but they don't enter the realm of the HIPAA privacy rule.

"It has nothing to do with HIPAA," said attorney Kirk Nahra, with WilmerHale, at The Virtual Thirtieth National HIPAA Summit[1] March 23. "HIPAA is not an overall health information privacy law. There have always been gaps in what was covered by HIPAA," which have become more apparent with the advent of mobile apps, wearables and patient support sites.

The success of the health care system depends on data and protecting its privacy, but organizations are running into complicated situations that weren't anticipated by the 2003 HIPAA privacy and security regulations. Although hospitals, insurers and clearinghouses are "reasonably comfortable with HIPAA rules," he said, "we are seeing tensions." One of the tensions involves patient access to their own data. For example, when patients receive information about their medical records and it moves from the provider through a mobile app, it's not regulated by HIPAA. "We have this tension in making it easier for patients to access," which may dilute the security, and "so far the decision has primarily favored access over security, but we are trying to make sure it's not a zero-sum game."

A huge quantity of identifiable health information is generated every day that isn't regulated by HIPAA, he said. "It doesn't mean the obligations are zero," but they're different. For example, the Apple Watch collects a broad range of information from patients, which is not subject to HIPAA, Nahra said. "Apple is not working for the hospital. It's not a covered entity or business associate and generally not subject to HIPAA," he said. But Apple also partners with insurers on an app that rewards enrollees for healthy behaviors (e.g., exercise). The app nudges enrollees who sign up to get their flu shot and take their medicine, he said. "That's an example of how alternate privacy rules matter." Aetna is probably in a position to handle the privacy requirements, but if a startup company develops the watch, there will have to be a way to address the gaps in privacy oversight.

One possibility is a broad, national privacy law, which may or may not have a HIPAA carve-out, Nahra said. "We are having a more active debate on national privacy legislation than we have in 20 years," although there won't be a law this year. There's more than a 50% chance of a national privacy law during the Biden administration, however, which is "more interested in a privacy law than the last administration," Nahra said. There are also comprehensive state privacy laws: the Virginia Consumer Data Protection Act, which was signed into law March 2, and the California Consumer Privacy Act. "So far, they apply to data that isn't protected by any other specific law," including HIPAA, Nahra explained.

Also, some data practices are subject to Federal Trade Commission (FTC) enforcement, which is expected to be more aggressive under the Biden administration, he said. "Both the FTC and state attorneys general have concerns about health data that isn't regulated by the HIPAA rules," Nahra said.

FTC Settles With Health Care App

Already there have been several FTC enforcement actions that foreshadow more activity in the health care space. For example, Flo Health Inc., the developer of a period and fertility-tracking app used by 100 million consumers, in January settled FTC allegations that it "shared the health information of users with outside data analytics providers after promising that such information would be kept private," according to an FTC press release.[2] In the settlement, Flo Health is required to obtain the consent of app users before sharing their health information and arrange an independent review of its privacy practices. Flo Health also is "prohibited from misrepresenting the purposes for which it or entities to whom it discloses data collect, maintain, use, or disclose the data."

The FTC's bite isn't in the form of fines. "The primary law they are working under passed in 1912, and it doesn't give them the ability to [impose] civil monetary penalties," Nahra explained. The century-old law allows the FTC to take action against unfair and deceptive trade practices (i.e., order the organization to cease and desist). "The FTC is looking at how it can be more effective in general and more aggressive in its remedies" despite the underlying statute. Its purview doesn't include nonprofits, he added.

Nontraditional uses of data by health care organizations and tech companies also raise eyebrows. "Health care systems are looking for all kinds of data on patients and collecting information on income, marital status and shopping patterns, and we're seeing the continued expansion of tech companies into the health care space," he noted. "At the same time, we are seeing all kinds of questions raised when data is regulated by HIPAA."

For example, in 2019, *The Wall Street Journal* reported[3] that hospital chain Ascension was partnering with Google in Project Nightingale. The health system will use Google's cloud platform and G-Suite patient records, which allows Google to have access to patient records from Ascension hospital patients in 21 states. As of February 2021, Project Nightingale is alive and evolving, according to STAT.[4]

Contact Nahra at kirk.nahra@wilmerhale.com.

1 Kirk Nahra, "Mini-Summit 4: Top Five Health-Care Privacy, Security Developments to Watch in 2021," The Virtual Thirtieth National HIPAA Summit, March 23, https://hipaasummit.com/.
2 Federal Trade Commission, "Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations that It Misled Consumers About the Disclosure of their Health Data," news release, January 13, 2021, https://bit.ly/320pOlW.
3 Rob Copeland, "Google's 'Project Nightingale' Gathers Personal Health Data on Millions of Americans," *The Wall Street Journal*, November 11, 2019, https://on.wsj.com/2Og1vdX.
4 Erin Brodwin, "Google expands controversial pilot project using patient data," STAT, February 23, 2021, https://bit.ly/3cZH4Ow.