wiley

NEWSLETTER

New York Attorney General Addresses Key Health Care Privacy Gaps

April 2017

The most important health care privacy cases so far this year emanated not from Washington, but from Albany. New York Attorney General Eric Schneiderman announced on March 27, 2017, that his office had reached settlements with three different health mobile applications, based on misleading claims and inappropriate privacy practices. These cases begin to fill in various gaps in the regulatory structure for privacy, and also present the possibility that state attorneys general may step up to fill an enforcement void if Washington pulls back on privacy and security enforcement across the Administration (and may become stronger actors regardless of Washington activity).

Practice Areas

Privacy, Cyber & Data Governance

The Cases

Following a year-long investigation, the attorney general (AG) announced three settlements against the following companies (as described in the AG press release):

- Cardiio, an American company that sells Cardiio, an app downloaded hundreds of thousands of times that claims to measure heart rate. The developer had not tested its accuracy with users who had engaged in vigorous exercise, despite marketing the app for that purpose. The developer also misleadingly implied that the app was endorsed by the Massachusetts Institute of Technology (MIT).
- Runtastic, an Austria-based company that sells Runtastic, an app that purports to measure heart rate and cardiovascular performance under stress. Yet the developer failed to test its accuracy with users who had engaged in vigorous exercise, despite marketing the app for that purpose to the 1 million

people who downloaded it.

- Matis, an Israel-based company that sells My Baby's Beat, an app downloaded hundreds of thousands of times, which Matis previously claimed could turn any smartphone into a fetal heart monitor, despite the fact that it has never been approved by the U.S. Food and Drug Administration (FDA). Although Matis exhorted consumers to use My Baby's Beat rather than a fetal heart monitor or Doppler, it never conducted, for example, a comparison to a fetal heart monitor, Doppler, or any other device that had been scientifically proven to amplify the sound of a fetal heartbeat.

Concerns and Authorities

While each settlement was based on its own facts, the AG's office focused on three separate areas of concern. First, the AG was concerned about the accuracy of various health claims made by the apps. The developers generally agreed to provide additional information about testing of the apps and to change their ads to make them non-misleading. Second, because these apps are not regulated by the FDA, the settlement required the apps to post clear and prominent disclaimers informing consumers that the apps are not medical devices and are not approved by the FDA. Third, on the privacy front, the settlements required specific changes to privacy policies and practices. The app developers are now required to obtain affirmative consent to their privacy policies for these apps and disclose that they collect and share information that may be personally identifying (including users' GPS location, unique device identifier, and "de-identified" data that third parties may be able to use to re-identify specific users).

For the settlements, the AG relied on specific broad principles of New York law. In particular:

- The New York State Executive Law prohibits "illegal or fraudulent acts" in the conduct of any business, trade or commerce, and allows the OAG to institute a special proceeding for restitution, damages, and/or injunctive relief against any party which has committed such acts. N.Y. Exec. Law § 63(12).
- The New York General Business Law prohibits "deceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service" in New York State, as well as "false advertising in the conduct of any business," and authorizes the OAG to enjoin any such practices. N.Y. Gen. Bus. Law §§ 349 and 350.
- Marketing a Health Measurement App without substantiation of its accuracy and that it measures what it purports to measure, and without fully and clearly disclosing privacy practices, constitute deceptive business practices in violation of New York Executive Law § 63(12) and General Business Law §§ 349 and 350.

A Big Deal?

So, why is this a big deal? Three settlements, payment of $30,000, who cares besides these three companies?

State attorneys general have traditional authority to regulate potentially deceptive practices. Each of the apps involved in these settlements was accused of making misleading or inaccurate statements about various health care claims related to the apps. These settlements indicate that at least this state AG is watching these

representations, and that apps will be challenged if their claims exceed their facts.

New York also is acting in a regulatory gap related to FDA oversight. The FDA has current oversight over certain "medical devices," but the full scope of this authority is an ongoing source of debate. In any event, these apps did not trigger FDA scrutiny. The New York AG is taking steps to ensure that consumers understand that these apps are not medical devices and are not approved by the FDA – a transparency issue of importance to consumers in this area. The Matis settlement, for example, contained a requirement to include language stating "This app is NOT a medical device, has not been reviewed by the FDA, and is NOT intended as a replacement for medical advice of any kind."

On the privacy front, the AG also is stepping into a regulatory gap. While these apps collected a broad range of health care information, because no "covered entity" is involved (e.g., a health care provider or health plan), the HIPAA rules are not applicable to these apps. HIPAA is an important and broad privacy rule, but it is not a general medical privacy rule – it applies only where personal data flows through or on behalf of a covered entity. Direct-to-consumer apps fit into this gap, meaning that HIPAA does not apply. The New York AG is stepping in to take steps to ensure privacy protections related to these apps, in the absence of a formal regulation. It is possible that we will see this as a first step – much like the Federal Trade Commission (FTC) has done with data security – toward regulation through enforcement.

Specifically, the New York AG required these apps to:

- Obtain affirmative consent to their privacy policies;
- Disclose to consumers the risk that third parties, who receive aggregated or "de-identified" data from the apps in order to provide services to the apps or otherwise, may re-identify data about specific users. (The settlements state that "Although this data does not identify users personally, there is a risk that third parties who receive such data from [the apps] may reidentify specific users.")
- Prior to sharing any de-identified user information with third parties, the apps shall, in writing, request that such third parties not attempt to re-identify the information to any particular individual. (It is interesting to note that one of these settlements required the app to "request" this agreement, while the other two settlements required the apps to "in writing, secure the express written agreement" not to re-identify.)
- Disclose that the health data collected by the apps may not be protected by the HIPAA rules;
- "Establish and implement reasonable security policies and procedures designed to protect user information," which must be "appropriate to the nature and scope of [the apps'] activities and the sensitivity of the covered information," and review and update these policies as necessary, at least bi-annually.
- Accordingly, this potentially groundbreaking series of settlements created new rules for factual support for health-related claims, required additional transparency that apps are not regulated by the FDA or HIPAA, and imposed new privacy and security obligations on the creators of these apps.

- Obviously, all app developers need to pay close attention to these issues. We will watch for whether the New York AG continues to take action in this area (or in a broad variety of other "non-HIPAA" areas), and whether other state AGs will join this effort. On a broader level, we will be watching closely whether state AGs become a more prominent focus of attention on privacy and data security enforcement. They have broad authority – through general "consumer protection" authority that mirrors the authority of the FTC, authority to enforce data breach notification laws and even the HIPAA rules (through specific mandates created by the HITECH law). They have had this authority for a long time, but we have not seen it exercised much. These cases may signal an important change. Pay close attention to the state AGs and any future actions over the next several years.