ROPES & GRAY ALERT

Privacy & Data Security ▪ Digital Health

April 12, 2017

New York Attorney General Enters Digital Health App and Privacy Enforcement Fray: Announces Three Settlements with Health and Fitness App Providers' Due to Efficacy Claims and Privacy Practices

Attorneys
James S. DeGraw
Paul D. Rubin

On March 23, the New York Office of the Attorney General ("NY OAG") announced Assurances of Discontinuance ("Settlements") with three developers of health and fitness mobile apps. The Settlements appear to mark the NY OAG's first endeavor into investigating the efficacy claims and privacy practices of these types of apps. The Settlements are notable for, among other things, including requirements that the app providers (i) clearly state that their apps are not for medical use; (ii) cease collecting certain user information, such as device identifiers; (iii) obtain affirmative consent from users to collect and share other sensitive information; (iv) inform users that data collected by an app may not be protected under the Health Insurance Portability and Accountability Act ("HIPAA"); and (v) inform users that aggregated app data that does not identify users personally may be shared with third parties and that those third parties might be able to reidentify specific users.

The Heart & Fetal Heart Monitoring Apps

Two of the apps, known as Cardiio (provided by Cardiio, Inc.) and Runtastic (provided by Runtastic GmbH), were promoted as helping consumers monitor their heart rate using a phone's camera. Those apps were available in the Health & Fitness section of app stores, for free or a small fee, where the providers claimed the apps could turn an iPhone into a personal heart rate monitor. Both claimed that their app could accurately capture a person's heart rate, even after exercise. Cardiio also claimed it could estimate one's life expectancy using the data the app collected.

Neither Cardiio nor Runtastic required users to expressly consent to the app's data collection practices, appearing to rely on notice through making a privacy policy available and implied consent. Among other things, the Cardiio app could collect GPS information and Runtastic unique device identifiers. Neither expressly disclosed that fact. Runtastic also had a live tracking feature that could share your location with third parties.

The third app, known as My Baby's Beat-Baby Heart Monitor App, was provided by Matis Ltd. The app was the most popular paid app in the Apple App Store medical category in 2016, and had as its logo a baby inside a stethoscope. Using only a phone's microphone, Matis claimed in the Apple App Store that "you can listen to your baby's heartbeat and movements, just like a Fetal Heart Monitor." In the Google Play store, Matis claimed that "[i]nstead of buying a home Doppler you can turn your smartphone into a Fetal heart monitor, using ONLY the PHONE'S MICROPHONE and a pair of headphones."

The data the app collected included global unique device identifiers, user feedback, an engagement score, and recordings. Though a privacy policy was available to users of the My Baby's Beat app, the policy did not disclose that that information was collected. The policy did disclose that data might be shared on an aggregated basis, but did not disclose risks associated with that practice.

In pursuing these investigations and settlements, the NY OAG relied on NY statutes prohibiting "deceptive acts or practices in the conduct of business" and "false advertising in the conduct of any business." N.Y. Gen. Bus. Law §§ 349, 350. While the targets neither admitted nor denied the NY OAG finding, the NY OAG Settlement with each is premised on the NY OAG's claims that "[m]arketing a Health Measurement App without substantiation that it accurately measures what it purports to measure, and without fully and clearly disclosing privacy practices, constitute deceptive trade practices." The NY OAG's allegations regarding both parts of this allegation are noteworthy. The first part – regarding claims of what the app can accomplish – stands as a warning itself for all providers of Life Style or Health & Fitness apps to ensure claims indeed are accurate. The second part – regarding data collection practices – if continued to be pressed by the New York and OAG, could result in a significant change in app data collection and sharing practices.

The Advertising Claims

With respect to the app providers' claims, the NY OAG in each Settlement noted that heart and fetal heart rate monitors generally are regulated as Class II medical devices by the FDA. Class II devices are higher risk devices than Class I devices, and "require greater regulatory controls to provide reasonable assurance of the device's safety and effectiveness."

The NY OAG alleged that claims made by Cardiio and Runtastic conveyed a "net impression" that the applications could accurately measure and monitor heart rates of users engaged in vigorous exercise – akin to heart rate monitors. But the applications did not provide sufficient evidence to substantiate such claims. In fact, it was not clear that the applications had been tested on users engaged in vigorous exercise.

As for the My Baby's Beat app, the NY OAG alleged that Matis informed users they could use My Baby's Beat instead of a fetal heart monitor or Doppler device. This claim was made despite the absence of FDA approval or clearance, and despite Matis not having conducted testing to compare its application to fetal heart monitors or Doppler devices. The New York OAG found all three apps could potentially harm consumers by providing inaccurate or misleading results.

In the Settlements, each of the app providers agreed to provide clear and prominent warnings. Matis revised its descriptions on app stores to state that My Baby's Beat app is not to be used for medical decisions of any kind. The providers of the heart monitor apps added warnings that those apps are not for medical use, and not cleared or approved by the FDA. As for the fetal heart monitor app, the provider also changed the name and logo of the app, and agreed to move the app from the "Medical" to "Lifestyle" app category.

The Privacy Claims

All three apps had privacy policies that appeared to rely on consumer consent by default. The Settlements state that the heart rate monitor app providers "maintain[ed]" privacy policies while the fetal heart monitor app providers made a privacy policy "available" to users. None appear to have required express user consent.

The NY OAG also found individual data handling and disclosure practices by the app providers troubling under New York's consumer deception laws. Cardiio, for instance:

i. could collect GPS location "which, when combined with other information about a user, may be personally identifiable information";

ii. could disclose aggregated data to third parties, but failed to disclose "the risk that third parties who receive such data . . . may reidentify specific users"; and

iii. did not disclose that "personal health information" (such as heart-related conditions) collected, stored and shared by Cardiio "may not be protected under the Health Insurance Portability and Accountability Act ('HIPAA')."

The Runtastic and Matis apps collected device identification information, which the New York OAG termed "personally identifiable information" in those Settlements.

In support of its claims that the risk of reidentification of aggregated data should be disclosed, the NY OAG in each Settlement cites papers by Prof. Paul Ohm and Prof. Latanya Sweeney that cast doubt on the efficacy of anonymization techniques, especially among combined data sets. *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010); Latanya Sweeney, *Only You, Your Doctor, and Many Others Know*, Technology Sci. (2015).

The NY OAG also criticized a statement in the Cardiio privacy policy that it could disclose user information to third parties if it believed in good faith that disclosure was "reasonably necessary to protect the property or rights of Cardiio, third parties or the public at large." The Cardiio Settlement states that "[t]his conferred virtually unlimited discretion on Cardiio, Inc. in disclosing users' personal information."

In the Settlements, the heart monitor app providers agreed to obtain express consent to their data handling practices from users. This includes requiring a user to scroll through the policy and affirmatively click on a consent button. The Cardiio policy going forward needs to, among other things, clearly and prominently disclose the above risks. Runtastic made similar commitments, as well as agreeing to adopt a right-to-be-forgotten mechanism. Matis, the fetal heart monitor app provider, among other things, agreed to stop collecting user device ids.

Take-Aways

The NY OAG's actions exemplify the increased enforcement risk for app providers from state attorneys general and other non-federal regulatory actors. With respect to health-related mobile apps, the NY OAG estimates there are more than 165,000 such apps available for download on smartphone devices. Many of these app providers are not covered by HIPAA and may presume (often incorrectly) that they are immune from FDA or state enforcement.

While the Federal Trade Commission ("FTC") has also shown interest in regulating this space, these recent NY OAG Settlements may represent a shift from federal agencies to state attorneys general in the regulation of claims and data handling procedures made by health-related apps. Although questions remain concerning the FTC's ability to regulate privacy practices under Section 5 of the Federal Trade Commission Act, the NY Attorney General, Eric T. Schneiderman, stated in announcing the Settlements that his office would "not hesitate to take action against developers that disseminate unfounded information that is both deceptive and potentially harmful to every day consumers."

Going forward, mobile app and software developers should evaluate how individual states could monitor their claims and privacy practices in addition, or in lieu of, federal regulators. Companies operating in health-related fields especially should review the claims they disseminate and the way they engage with consumer privacy data in light of the ever-developing regulatory environment.

To discuss these settlements and strategies relating to consumer protection and privacy policies, please contact your regular Ropes & Gray Digital Health or FDA contact.

Links:

In re: *Cardiio, Inc.*, Assurance No.: 16-173

In re: *Matis Ltd.*, Assurance No.: 16-101

In re: *Runtastic GmbH*, Assurance No.: 16-174