

Think Before You App: FTC Releases Compliance Tools for Health App Developers

Kelley Drye

April 11, 2016

The Federal Trade Commission furthered its outreach to the mobile app developer community last week by issuing new guidance for integrating privacy and security into mobile health apps, as well as an interactive online tool for determining whether key laws apply. As referenced in Consumer Protection Bureau Director Rich's [testimony a few weeks ago](#), the FTC has been working with a number of other agencies to address concerns about collection, storage, and use of consumer health information in light of the proliferation of consumer-directed health technology and consumers' engagement in this area.

To use [the tool](#), developers answer a series of high-level questions about the nature of their app, including about its function and the data it collects. Based on the answers to those questions, the tool advises the developer about whether the FTC Act, the FTC's Health Breach Notification Rule, HIPAA, or the Federal Food, Drug and Cosmetic Act likely applies to the app. In some cases, the tool links out to other guidance that may be relevant for the app, such as FTC's [guidance for complying with the Health Breach Notification Rule](#). The FTC developed the tool in conjunction with the Department of Health and Human Services' Office of National Coordinator for Health Information Technology, Office for Civil Rights and the Food and Drug Administration.

Along with the tool, the FTC released recommended [best practices for privacy and security in mobile health apps](#). The guidance encourages developers to minimize the information their apps collect, to limit and control access to the apps and to the data they collect, and to implement "security by design." This health-app-specific guidance builds upon the FTC's [general guidance](#) for mobile app developers. For those developing apps, FDA's policies regarding [whether such apps are regulated as medical devices should also be considered](#).

The main lesson that is underscored in all of these tools is the same: Consider the nature of the information collected and its potential use at the concept phase and rather than after development is complete. All too often, as companies rush to submit apps for approval on an app store, legal compliance is an afterthought. As we have learned from the 100+ privacy and data security settlements that the FTC has released, these issues can be very difficult to cure on the back end.