Published on *The National Law Review* https://natlawreview.com

FTC Releases Online Tool to Help Health App Developers Identify Applicable Laws

Article By:

Dena Feldman

Christina G. Kuhn

On April 5, the ***Federal Trade Commission (FTC)***, in conjunction with the ***Food and Drug Administration (FDA)*** and the ***Department of Health and Human Services (HHS)***, released a new web-based interactive tool to assist mobile health app developers in navigating applicable federal laws and regulations in the areas of advertising and marketing, medical devices, and data security and privacy.

The interactive tool consists of 10 questions designed to identify whether a particular mobile health app is subject to any of the following federal laws:

- the privacy, security and breach notification rules issued under the Health Insurance Portability and Accountability Act (HIPAA);
- the Food, Drug, and Cosmetic Act (FDCA);
- the Federal Trade Commission (FTC) Act; and
- the breach notification rules issued by the FTC.

Regardless of whether mobile apps are subject to any of these federal laws, the guidance directs app developers to newly issued FTC best practices for protecting the privacy and security of consumer data.

Health Privacy Laws (HIPAA)

The interactive tool mainly repeats what HHS has already said regarding HIPAA's application to mobile apps: HIPAA applies to mobile health apps that are developed by HIPAA covered entities (such as a health care provider or health plan) or by business associates who create, receive, transmit, or maintain protected health information on behalf of a HIPAA covered entity. The tool also notes that an app that requires a physician's "prescription" may render the developer a health care

provider, and therefore subject to the requirements of HIPAA.

The application of HIPAA to mobile apps has received much attention over the past few months. In October 2015, the Office for Civil Rights at the U.S. Department of Health and Human Services (OCR) released an online health app developer portal seeking questions from mobile health application developers regarding HIPAA's implications for mobile health applications. In February 2016, OCR released further guidance on when an app developer would be required to comply with HIPAA and whether HIPAA would apply to health information stored on a mobile app. OCR set forth several different scenarios and analyzed whether HIPAA would apply to each. OCR concluded that HIPAA does not apply to most direct-to-consumer apps, i.e., when patients download mobile health apps on their own volition, populate their own information into the app, and do not transmit such information back to a covered entity. However, if a covered entity contracts with an app developer, and the app integrates information from the patient's electronic health record, or transmits information back to the provider for clinical monitoring or patient management services, then HIPAA likely would apply.

Still, some Members of Congress have continued to express their frustration and belief that HHS is lagging behind the demand for patient access to new technology, calling the recent OCR efforts inadequate.

Food and Drug Administration Requirements

The interactive tool includes three broad questions to assist users in determining whether FDA would regulate an app under the FDCA, asking the user to identify (1) whether the app meets the statutory definition of a "device" in the FDCA; (2) whether the app pose only "minimal risk," in which case FDA would not enforce compliance with the FDCA; and (3) whether the app meets the definition of "mobile medical app" that is the focus of FDA's regulatory oversight.

FDA previously described its regulatory approach to mobile apps in a 44-page guidance document . Other aspects of FDA's approach to software tools are described in other sources, such as the Health IT Report. By attempting to distill these lengthy and detailed sources of guidance into three broad questions, the interactive tool could result in users failing to appreciate many of the more difficult and subtle issues in determining whether an app will be regulated by FDA. For example, the threshold question of determining whether an app meets the definition of a medical device can be a complex issue, particularly for software tools that help physicians or patients manage diseases or conditions or make health-related decisions. The other two questions addressed by the interactive tool are similarly complicated.

App developers and other users should therefore consult FDA's guidance and other resources when working through the interactive tool.

Federal Trade Commission Rules and Best Practices

The interactive tool notes that the FTC Act would not apply to a developer that is a non-profit organization. Furthermore, mobile medical apps may implicate FTC's health breach notification rules when such apps offer health records directly to consumers, or interact with or offer services to someone who does. In such cases, an app developer may be considered a personal health records (PHR) vendor, a PHR-related entity, or a service provider that must comply with FTC's health breach notification rule (The FTC breach notification rule does not apply to HIPAA covered entities, which are subject to the HIPAA breach notification rule.)

Even if the interactive tool does not identify any federal laws applicable to a medical mobile app, the FTC still offers guidance for developers. The FTC released new "Best Practices" for all medical mobile apps. The FTC advises all mobile health app developers to consider implementing the following safeguards:

- *Minimize data.* Retain individualized information only if it is needed and store information in de-identified form when possible.
- *Limit Access and Permissions.* Allow the app to access only needed customer information, use a trusted user interface, and make sure settings default to protect user privacy.
- *Keep Authentication in Mind.* Implement strong user authentication requirements (e.g., pair strong passwords with text and email codes), store passwords securely, and limit access to data or functionality to clients or parties with a legitimate need.
- *Consider the Mobile Ecosystem.* Assess the security of the mobile platform, third-party service providers, and code developed by third parties.
- *Implement Security by Design.* Implement a culture of security: incorporate data security at every stage of the app's lifecycle, protect from common vulnerabilities, update software to maintain the latest security protections, inventory and track data collected and retained by the app.
- *Don't Reinvent the Wheel.* Take advantage of what experts have already learned about security by using free and low-cost tools to safeguard consumers' personal information.
- *Innovate How You Communicate with Users.* Get users' consent before collecting or sharing consumer data, implement an informative and accessible privacy policy, and inform users about the app's security features.
- *Don't Forget About Other Applicable Laws*. Even if HIPAA, the FDCA, or the FTC Act do not apply, consider whether other laws, such as the Children's Online Privacy Protection Act (if the app collects information from children) or the Gramm-Leach-Bliley Act (applicable to financial institutions), may apply. Furthermore, consider applicable state laws and "basic truth-in-advertising and privacy principles."

The new interactive tool will likely be helpful in providing mobile app developers who are working in the health, wellness and medical areas with a means of considering, at a very high level, the various federal laws that may be applicable to their technologies. As noted above, these developers should be mindful, however, that the interactive tool is intended to address and simplify several extensive bodies of law and, of necessity, does not address numerous nuances and ambiguities in the laws that may affect how the laws apply in any particular situation.

National Law Review, Volume VI, Number 98