FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

MOBILE HEALTH APPS INTERACTIVE TOOL

Produced in cooperation with the U.S. Department of Health & Human Services (HHS): the Office of the National Coordinator for Health Information Technology (ONC), the Office for Civil Rights (OCR), and the Food and Drug Administration (FDA)

The Office of the National Coordinator for Health Information Technology
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE FOR CIVIL RIGHTS
FDA

TAGS: Advertising and Marketing | Health Claims | Privacy and Security | Consumer Privacy | Data Security | Tech | Health Care

You're developing a health app for mobile devices and you want to know which federal laws apply. Check out this interactive tool.

What are the Laws?

Does your mobile app collect, create, or share consumer information? Does it diagnose or treat a disease or health condition? Then this tool will help you figure out which – and it may be more than one – federal laws apply. It's not meant to be legal advice about all of your compliance obligations, but it will give you a snapshot of a few important laws and regulations from three federal agencies.

Health Insurance Portability and Accountability Act (HIPAA)

The Office for Civil Rights (OCR) within the U.S. Department of Health & Human Services (HHS) enforces the HIPAA rules, which protect the privacy and security of certain health information and require certain entities to provide notifications of health information breaches.

Federal Food, Drug, and Cosmetic Act (FD&C Act)

The FDA enforces the FD&C Act, which regulates the safety and effectiveness of medical devices, including certain mobile medical apps. The FDA focuses its regulatory oversight on a small subset of health apps that pose a higher risk if they don't work as intended.

Federal Trade Commission Act (FTC Act)

The FTC enforces the FTC Act, which prohibits deceptive or unfair acts or practices in or affecting commerce, including those relating to privacy and data security, and those involving false or misleading claims about apps' safety or performance.

FTC's Health Breach Notification Rule

The FTC's Health Breach Notification Rule requires certain businesses to provide notifications following breaches of personal health record information.

WHICH LAWS APPLY TO MY MOBILE HEALTH APP?

1. Do you create, receive, maintain, or transmit identifiable health information?

YES

GO TO QUESTION 2 to determine if HIPAA applies.

NO

2. Are you a health care provider or health plan?

YES

NO

GO TO QUESTION 3 to see if HIPAA applies.

3. Do consumers need a prescription to access your app?

YES

NO

GO TO QUESTION 4 to see if HIPAA applies.

4. Are you developing this app on behalf of a HIPAA covered entity (such as a hospital, doctor's office, health insurer, or health plan's wellness program)?

YES

NO

You likely are not covered by HIPAA.

GO TO QUESTION 5 to see if the FD&C Act applies.

5. Is your app intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment or prevention of disease?

YES

NO

The FD&C Act does not apply. Your app is not considered a medical device and is outside of FDA purview. For examples of mobile apps that are not medical devices, *see* Appendix A of the FDA's Mobile Medical Applications Guidance for Industry and Food and Drug Administration Staff [PDF].

GO TO QUESTION 8 to see if the FTC Act applies.

6. Does your app pose "minimal risk" to a user?

According to the FDA, "minimal risk" apps are those that are **only** intended for one or more of the following:

- helping users self-manage their disease or condition without providing specific treatment suggestions;
- providing users with simple tools to organize and track their health information;
- providing easy access to information related to health conditions or treatments;
- helping users document, show or communicate potential medical conditions to health care providers;
- automating simple tasks for health care providers;
- enabling users or providers to interact with Personal Health Records (PHR) or Electronic Health Record (EHR) systems; and
- transferring, storing, converting format or displaying medical device data, as defined by the FDA's Medical Device Data Systems regulations.

YES

The FDA considers your app to be of minimal risk, and does not intend to enforce compliance with its regulatory requirements.

GO TO QUESTION 8 to see if the FTC Act applies.

For additional information about mobile apps over which the FDA intends to exercise enforcement discretion, *see* Appendix B of the FDA's Mobile Medical Applications Guidance for Industry and Food and Drug Administration Staff [PDF].

NO

7. Is your app a "mobile medical app?"

A "mobile medical app" is one that is intended for any of the following:

- use as an accessory to a regulated medical device (for example, an app that alters the function or settings of an infusion pump)
- transforming a mobile platform into a regulated medical device (for example, an app that uses an attachment to the mobile platform to measure blood glucose levels)
- performing sophisticated analysis or interpreting data from another medical device (for example, an app that uses consumer-specific parameters and creates a dosage plan for radiation therapy)

YES

NO

Please contact the FDA at mobilemedicalapps@fda.hhs.gov to determine if you need to comply with the FDA's regulatory requirements.

GO TO QUESTION 8 to see if the FTC Act applies.

8. Are you a nonprofit organization?

YES

NO

It's likely that the **FTC Act** applies.

GO TO QUESTION 9 to see if the FTC's Health Breach Notification Rule also applies.

The FTC Act

The FTC Act prohibits deceptive or unfair acts or practices. This means:

- You cannot make deceptive or misleading claims to consumers about things that are important to them; and
- You cannot engage in acts or practices that cause, or are likely to cause, substantial injury to consumers that they cannot avoid, and that do more harm than good.

Here are some tips for how to protect consumers' privacy and the security of their data. Here is some guidance for how to ensure your health benefit, safety, performance, and other claims are truthful, substantiated, and not misleading.

9. Are you developing this app as or on behalf of a HIPAA covered entity (such as a hospital, doctor's office, health insurer, or health plan's wellness program)?

YES

NO

GO TO QUESTION 10 to see if the FTC's Health Breach Notification Rule applies.

10. Do you offer health records directly to consumers (or do you interact with or offer services to someone who does)?

YES

NO

The FTC's Health Breach Notification Rule does not apply.

You've completed this interactive tool.

We hope this tool has helped you figure out which federal laws may apply to your mobile health app. No matter which laws apply, consumers want your app to be safe and secure. Here are some tips for how to protect consumers' privacy and the security of their data.

Glossary

Identifiable health information

Identifiable health information includes demographic information and relates to a consumer's past, present, or future physical or mental health or condition; the provision of health care; or the past, present, or future payment for provision of health care to the consumer, that identifies the consumer or for which there's a reasonable basis to believe it can be used to identify the consumer. For example, the consumer's IP address, if maintained by a health plan's wellness app, is identifiable health information.

^ top

HIPAA covered entities

Health care providers who conduct certain electronic transactions*

Covered health care providers include doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies that conduct certain payment and coverage related health care transactions electronically. Providers range

from small physician practices to large hospital systems.

Health plans*

Health plans include health insurance companies; HMOs; company health plans; and government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans' health care programs.

Health care clearinghouses*

Health care clearinghouses are entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa. For example, entities that process health information by standardizing and sending claim information from providers to insurance payers are health care clearinghouses.

*For more information, *see* Are You a Covered Entity?; Covered Entity Charts [PDF].

^ top

HIPAA business associate

A business associate creates, receives, maintains or transmits protected health information as it performs certain functions or activities on behalf of, or provides certain services to, a covered entity. These functions or activities include claims processing, data analysis, utilization review, and billing. Business associates include a person that provides data transmission services with respect to PHI that requires access to the information on a routine basis, as well as a person that offers a personal health record on behalf of a covered entity, and a subcontractor to another business associate. For more information on business associates, *see*:

OCR's Health App Developer Portal

Health Information Privacy, Understanding HIPAA Privacy for Covered Entities and Business Associates;

Health Information Privacy, Business Associates, Frequently Asked Questions; and

Health Information Privacy, Understanding HIPAA Privacy for Covered Entities and Business Associates, Sample Business Associate Agreement Provisions.

^ top

Protected health information (PHI)

Identifiable health information maintained or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

^ top

Medical device

A medical device is an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is:

recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them,

intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or

intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of any of its primary intended purposes.

^ top

Mobile medical app

To determine if you are a mobile medical app, see Section V.A. of the FDA's Mobile Medical Applications Guidance for Industry and Food and Drug Administration Staff [PDF] ("Mobile medical apps: Subset of mobile apps that are the focus of FDA's regulatory oversight") to identify the types of apps that FDA intends to oversee actively, and see Appendix C of the FDA's Mobile Medical Applications Guidance for Industry and Food and Drug Administration Staff [PDF] ("Examples of mobile apps that are the focus of FDA's regulatory oversight (mobile medical apps)"), which provides examples of apps that are mobile medical devices. You can also visit the Mobile Medical Applications website.

If you have further questions in determining whether your app is a medical device, email mobilemedicalapps@fda.hhs.gov or contact the FDA via Device Advice: Comprehensive Regulatory Assistance; CDRH Division of Small Manufacturers, International and Consumer Assistance (DSMICA).

^ top

Personal health records (PHR) provider, PHR-related entity, or service provider

PHR provider

A PHR provider offers PHRs – electronic health records that can be drawn from multiple sources and that are managed, shared, and controlled primarily by or for the individual – directly to consumers.

PHR-related entity

A business that interacts with a PHR vendor, either by offering products or services through the vendor's website (regardless of whether that vendor is covered by HIPAA), or by accessing information in, or sending information to a PHR.

Service Provider

A business that offers services to a PHR vendor or PHR-related entity involving the access, use, maintenance, modification, disclosure, or disposal of health information.

^ top

April 2016