

Mobile Health Apps Legal Compliance Essentials for FDA and FTC Standards

May 22, 2025

By Michael H. Cohen

Apps that provide services such as telemedicine, fitness tracking, remote monitoring, and medication reminders are rapidly expanding within the burgeoning mobile health (mHealth) industry. But with this growth comes an increase in regulatory scrutiny. Developers, healthcare providers, and startups in this space need to be on guard because the law is looking much more closely at the nascent mHealth industry. And a lot of the apps we're developing are now being classified as medical devices, with some of us on the borderline of telemedicine.

This manual will take you through the basic legal factors involved in mobile health apps. It will help you figure out if your app is regulated by the FDA, how to manage patient data in a way that meets the requirements of HIPAA, and how to ensure that your app's advertising practices are in line with FTC guidelines. You will also learn about state laws—in particular, telehealth and privacy laws—that may impact the operation of your app.

1. Determining If Your App Needs FDA Approval

When a mobile health app meets the definition of a medical device according to 21 CFR 801, the FDA gets involved. If your app is intended to diagnose, treat, or prevent a disease or health condition, it likely comes under FDA oversight. Apps that are concerned only with general wellness or non-medical functions are usually not directed by the FDA.

For instance, an application that measures blood pressure and works together with a medical device or one that employs AI to evaluate skin conditions might be classified as a medical device and need to meet FDA requirements. However, step counting apps or those promoting meditation generally do not require such measures.

The complete guidance from the [FDA](#) can be reviewed.

To avoid FDA regulation, think about these strategies:

- State clearly that your app is not intended to diagnose or treat any medical conditions.
- Ensure that any connected devices are already FDA-approved.
- Don't use promotional language that suggests your app can prevent, diagnose, or treat disease.

2. Complying with HIPAA When Handling Patient Data

If your app gathers, holds, or communicates protected health information (PHI), compliance with the Health Insurance Portability and Accountability Act (HIPAA) is a must. This is especially true if your app works with electronic health records (EHRs), collects medical histories or test results, or corresponds with healthcare providers in its user communications.

Determine whether your application qualifies as a HIPAA-covered entity.

To satisfy HIPAA mandates, you must encrypt stored data and data in transit. When you're using cloud platforms, choose from those that are HIPAA-compliant—the Amazon Web Services (AWS) platform is well-known for this, as is the Google Cloud Healthcare API. Always get consent from users before you collect or share their health data. And for good measure, implement multi-factor authentication to ensure that only authorized users can access your systems.

Learn more about how the Security Rule of HIPAA applies to mobile health applications.

3. Staying Compliant with FTC Marketing Rules

When you assert that your app has capabilities that can affect the health of its users, you must be certain that those assertions are accurate, and supported by solid evidence. The Federal Trade Commission keeps a close eye on the marketing of health-related matters and does not shrink from taking action against misleading or overstated assertions.

Common pitfalls consist of not stating clearly the actual effectiveness of the app (e.g., saying it cures insomnia), using testimonials and not having scientific backing to use them, and not disclosing connections between the app developers and the influencers or endorsers of the app.

View the complete guidance issued by the FTC on the marketing of health products.

An instance that is very well known is the FTC's case against Lumosity in 2015. The company ended up having to pay \$2 million because it had made dubious claims that its brain training games could stave off cognitive decline. For details, see this page.

To prevent this type of enforcement, ensure that you support health claims with rigorous scientific research; include disclaimers when necessary, and always disclose any financial or promotional relationships.

4. State Privacy Laws and Their Impact on Health Apps

Your app may still have obligations under state privacy laws even if HIPAA doesn't apply to it. Laws protecting consumer data and imposing requirements on businesses collecting personal health information have been enacted in several states.

For instance, the Consumer Privacy Act (CCPA) of California underscores the need for transparency and grants users the authority to refuse permission for the collection of their data.

New York's SHIELD Act mandates that companies implement sensible security practices to protect the information of their customers.

Illinois' Biometric Information Privacy Act (BIPA) regulates the gathering of biometric data, such as fingerprints and facial recognition.

For your app to remain compliant, it should have a prominent and plain privacy policy, should give users an option to not share data, and should make sure that all biometric data are encrypted and collected only after the user has consented.

To see privacy laws in various U.S. states, check this page.

5. Practical Steps for Legal Compliance

Assess your app and its functions for FDA oversight. If what you're doing is in any way similar to what an FDA-regulated company would do, then most likely you must comply with FDA regulations. The same logic applies to HIPAA (It's All About Compliance, 2021). Your app, if it handles protected health information in a manner similar to what a healthcare entity would do, must comply with HIPAA. Noncompliance can be very costly. The Federal Trade Commission (FTC) regulates truth in

advertising on a federal level. Your marketing efforts must be FTC-compliant.

See a list of recent enforcement actions taken by the [FTC and FDA](#) against mobile health apps.

Health mobile apps are in a highly regulated area, and not completing them can lead to serious legal problems—for instance, regulatory fines, consumers suing the company, or even removal of the app from the app stores. If you need help figuring out interaction with the FDA, HIPAA, FTC, or your state compliance for your health tech product, our legal team at Cohen Healthcare Law Group is here to help.