Clearwater

Whitepaper

Understanding Health Apps, HIPAA, and the FTC: How They're Connected & Why it Matters

Table of Contents

Introduction 3

What do we mean by health apps? 3

App adoption 5

Healthcare apps and legal frameworks 6

Apps and HIPAA 6

The FTC Act 7

FD&C Act 9

State and other applicable laws 9

Protect yourself, regardless of regulatory requirements 10

Introduction

Blood sugar monitors. Smartwatches. Heart monitors. Weight and exercise trackers.

In the last several years, healthcare has seen an explosion in the adoption and usage of smart and connected health devices and their apps, both from clinical and consumer users.

And while some of the device types and health-related data usage make it clear what's covered by HIPAA regulations, many healthcare providers may not know that when it comes to these devices and apps, there is a range of regulations, reporting requirements, and monitoring agencies that extend well beyond HIPAA's scope.

Unfortunately, many healthcare-covered entities and their business associates struggle to understand which apps require which governance and how to develop appropriate privacy and security policies to meet changing and expanding requirements.

In addition to HIPAA, some of these apps may be subject to Federal Trade Commission (FTC) Act requirements, while others may fall under the Food, Drug and Cosmetic Act (FD&C) Act, and for some, it's all three.

So, how do you know which regulations apply to the apps and devices used to support your healthcare organization's objectives? Let's look at some broad categories under which the apps and devices your organization may suggest your patients use may fall.

What do we mean by health apps?

While not all-encompassing, here are five categories of health apps and devices:

1. **Clinical and diagnostic assistance** - These apps and devices are often used within the healthcare organization to access digital health records. For example, electronic health records (EHR) and electronic medical records (EMR).
2. **Remote monitoring applications** - There has been a significant spike in telehealth services, primarily driven by the pandemic, for example, remote monitoring for blood pressure, glucose, heart rate, etc.

3. **Health apps for clinical reference** - These apps generally assist clinicians with tasks such as medical coding, dictionaries, and other information sources.
4. **Productivity apps** - These apps generally help automate processes associated with billing, record keeping, prescribing, and other similar provider-focused activities.
5. **Healthy lifestyle apps** - These app types are generally consumer-focused; they track physical activity such as how many steps a person takes, heart rate during the day, quality of sleep, etc.

While these categories help paint a picture of some of the common applications providers and consumers use in healthcare today, it's important to note that not every app falls into one of these distinct categories.

And as healthcare evolves to keep up with digital health adoption, we're also seeing the lines blur between these categories.

For example, an app that the payer community might provide might give a consumer access to information about their healthcare. Still, it might also include a wellness program that culls information about healthy lifestyles.

Or, a provider might recommend an app for patients to access their EMRs. We see increased APIs to allow for third-party access in response to healthcare interoperability rules. When consumers download an app from an app store, they can use that app to connect with a healthcare provider, pull in medical record information, and pair that information with information from a healthy lifestyle app.

These examples blur the lines between app-type categories, and as additional features become available within the apps, more and different data source types get pulled in. Some of these could be from non-traditional healthcare organizations, for example, Apple Health, Google, or others.

It's not just commercial software developers getting on board. More medical device suppliers are getting involved in health app creation, too. Today, medical devices are either software as a medical device itself, software embedded within a medical device, or software in a medical device. For example, devices like infusion pumps and similar devices often have software included or can be controlled through software applications.

As a result, it's more challenging for healthcare organizations and business associates to clearly understand the legal structure and regulations that apply to different apps.

Even more challenging is that it's no longer just about the cybersecurity of those devices. There are also growing concerns about the security and privacy of the data types those devices collect, store, and transmit. This can include sensitive information such as personally identifiable information (PII) to more protected information such as personal health information (PHI) or financial information.

App adoption

Healthcare app adoption has been exponential, especially between 2020 and 2021.

While there has been a significant investment in digital health and telehealth in healthcare app adoption, specifically at a consumer level, it stalled a bit before the coronavirus pandemic.

For example, a survey by Accenture indicated that between 2016 and 2018, mobile health apps increased from 33% to 48%, but that dropped to 35% in 2020, the first year of the pandemic. Likewise, wearable technologies decreased in 2020 to 18% from 21% just two years before.

However, COVID-19, according to the report, forced a surge in both app usage and wearables.

Yet, consumers remain cautious about these apps and devices, particularly regarding security and data privacy. Many noted that security and privacy remain a top barrier to adoption, especially mobile app usage. That's created an uphill journey for medical device and app developers who must work harder to build consumer trust that their healthcare data will remain secure and private.

> The global mobile healthcare market is expected to reach almost $312 billion by 2027. What does that look like in terms of mobile health apps? According to the IQVIA Institute for Human Data Science's 2021 trends report, some 90,000 digital health apps were released in 2020, with an average release of 250 apps per day.

Healthcare apps and legal frameworks

As mentioned earlier, a range of legal and regulatory frameworks may govern the privacy and security of healthcare apps and devices. Here, we'll look at three of them, specifically HIPAA, the FTC Act, and the FD&C Act. However, it's worth noting that the market continues to evolve. New regulations are coming into play more frequently than ever before, not just at the industry level but also at the federal and state levels.

Electronic protected health information (ePHI) generally applies to healthcare-covered entities, business associates, and patients from a HIPAA perspective.

For the FTC, the focus is generally on third-party entities not generally covered by other agencies, including HIPAA. The data may look like ePHI, but it's usually something else not covered by HIPAA.

Finally, the FD&C Act generally applies to providers and medical device manufacturers specifically regarding the health data these devices store or use.

Apps and HIPAA

In terms of HIPAA, the application source and the information transmitted determines if HIPAA applies.

Information might include medical history, treatment, diagnostic, or payment information. In general, it's lots of data generated by healthcare providers, the payer community, and business associates.

A good question for consumers would be, "Did I download this app from my healthcare provider?" For example, through a link on a patient portal or from a link off of a payer's portal? If so, the HIPAA privacy and security rules may apply, specifically related to the administrative, technical, and physical safeguards needed to protect the confidentiality, integrity, and availability of ePHI. The breach notification rule may also apply.

It's important to note that the HIPAA Security Rule doesn't provide a prescribed list of controls an organization must have within a healthcare application. There are, however, some baseline controls that should be in place. Additionally, organizations should conduct a risk analysis to understand if additional controls are reasonable and appropriate to help manage risk associated with a breach of the confidentiality, integrity, and availability of information processed.

So, when does HIPAA apply?

Here is an example: If a consumer can go to a provider-patient portal and download a healthcare app, which allows access to medical records and communicate with providers, like asking questions or making appointments, ePHI may be involved. Even if the provider gets the application from a business associate working on behalf of the provider, HIPAA will likely apply.

On the other hand, if you're a healthcare provider and engage in an agreement with a business associate to build an app on your behalf, the app developer likely won't build an app exclusive to your practice. The developer will likely create the app and make it available through an app store to the public. When a consumer downloads the app, there is an option to connect to a provider through an API for EMR access. HIPAA would not likely apply here.

Why?

In both examples, the patient accessed their medical records using an identical app or essentially within an app. But in the first example, the consumer got the app directly from a provider, so HIPAA applies. In the second example, the consumer got the app directly from the app developer, so HIPAA doesn't apply. Specifically, it doesn't apply after that healthcare data leaves the API and goes into the application. So, HIPAA doesn't apply to the app developer in that example.

In the first example, the app developer was a business associate, so the Security Rule would apply to the app's development and to the extent it processes ePHI. It's important to note the fine line where the same information is used, but the application itself has different sources.

For HIPAA, it all comes down to these questions: Who is the application's source? Did it come directly from a healthcare-covered entity or a third party?

The FTC Act

The Federal Trade Commission (FTC) Act was adopted in 1914. Under this rule, the FTC, which is the nation's consumer protection agency, is empowered to, among other things, prevent deceptive and unfair acts or practices, seek monetary remedies or redress, institute rulemaking, and conduct investigations for compiling information and understanding what the best business practices are or could be.

In short, the FTC protects companies from misleading consumers or engaging in unfair practices.

Deceptive and unfair trade practices also apply to the security and privacy of healthcare applications. So does making representations about having specific privacy policies or security measures in place but not having them in place or representations about health data and protections that the FTC may conceive as unfair and deceptive trade practices.

Regarding the FTC Act, these are the types of things health app developers should be cognizant of when making representations about what their apps do.

Suppose the app developer is not covered by HIPAA or is not acting as a business associate under HIPAA. In that case, the developer should consider whether the FTC Act applies, which is likely in several instances where there is health data collection.

The FTC also issued a policy statement indicating that developers of health apps, connected devices, and similar products fall under this purview and must also comply with a Health Breach Notification Rule. Here, this relates to a personal health record, which is defined as an electronic record of identifiable health information on an individual that can be drawn from multiple sources, and then is managed, shared, and controlled by or primarily for the individual.

For example, an app is likely covered if it collects information directly from consumers. It then has the technological capacity to draw information from an API that enables syncing to a fitness app or similar tracker. In some cases, an app pulls data from multiple sources, like a blood sugar monitoring app that draws health information from a consumer's input of blood sugar levels, but also takes non-health information from another source such as a phone calendar and syncs them together. In this case, the app would be covered under the Health Breach Notification Rule.

There are also terms in the rule about which entities are covered: vendors of personal health records (PHRs), PHR-related entities, and third-party service providers.

Vendors of personal health records (PHR) offer or maintain a PHR and are usually not covered by HIPAA.

PHR-related entities are entities not covered by HIPAA that offer products or services through websites of HIPAA-covered entities that offer individuals PHI, access information in a PHR, or send that information to a PHR.

Third-party service providers are similar to business associates under HIPAA. They're providing services to a vendor in connection with offering maintenance of the PHR or to a related entity in connection with the product or service provided

by the entity, which accesses, maintains, modifies, records, stores, destroys, or handles unsecured PHR-identified health information as a result of providing these services.

For FTC purposes, a breach of security has a few triggers. One of them is the acquisition of unsecured PHR and identifiable health information of an individual in a PHR without an individual's authorization.

FD&C Act

The FD&C Act has implications for software as a medical device or software in a medical device. Whether or not the act applies depends on the intended use of the application and whether or not it will be used to diagnose, cure, or mitigate treatment or prevent disease.

If the app falls within this intended use, it may be covered under one of three classes of risk of the FD&C Act. The FDA defines medical devices in three classes: Class 1, Class 2, and Class 3, based on the potential impact on the patient or the user of the medical device and their health.

A Class 1 device has minimal impact; it may just be collecting information or helping users self-manage a disease or condition without providing specific treatment suggestions. The FDA may use enforcement discretion regarding a Class 1 mobile medical application. If an application makes recommendations or diagnostic suggestions, it's likely a Class 2 or 3, and developers need to be attuned to regulations that might be applicable under this Act.

Class 2 and Class 3 devices likely require the developer to undergo a regulatory process, including submission for pre-market risk analysis and associated security information.

State and other applicable laws

In addition to HIPAA, the FTC Act, and the FD&C Act, it's worth noting that a growing number of states are now passing their own data privacy and security laws. As such, it's essential to stay up-to-date on how these new requirements might affect mobile health apps and mobile health device development and use.

Additionally, the Children's Online Privacy Protection Act (COPPA) imposes specific requirements on operators, websites, or online services directed to

children younger than 13. There could also be applicable foreign laws, like GDPR.

Many changes are emerging from the federal level, including more push toward National Institute for Standards Technology (NIST) framework adoption for security and risk management.

Congress also recently passed legislation requiring owners and operators of critical infrastructure to report cyber incidents to the U.S. Department of Homeland Security and the U.S. Securities and Exchange Commission, which recently proposed a cybersecurity rule that may apply to registered investment advisors and registered investment companies.

Protect yourself, regardless of regulatory requirements

While this focus is primarily on mobile health apps and devices, it's important to remember that the bigger picture is about protecting health data vulnerable to cyberattacks and breaches.

Ideally, health apps are doing everything they can to proactively prevent breaches and ensure they can quickly identify, stop, and recover from any potential attacks.

So, when building a healthcare app, one of the best practices you can adopt is to build security into your software development lifecycle. When developers think backward and are forced to bolt on security measures after the fact, it's time and cost-consuming and can negatively impact operations and functionality. To ensure you're meeting all of your compliance and regulatory requirements out of the gate, include them in the development of the application from the get-go.

As this becomes an integral part of your software development lifecycle, you'll want to be sure that your teams address and manage risks on an ongoing basis, specifically as it applies to HIPAA requirements and security and privacy best practices.

Understanding your organization's risk threshold or register is critical to this process. Hence, your team knows in the earliest stages of your software development lifecycle which risks meet or exceed what has been deemed reasonable or appropriate—this requires a risk assessment. This critical risk management activity also helps you identify additional safeguards and security controls to help minimize risks that meet or exceed your risk threshold.

It's also important to routinely test your team's controls to ensure your safeguards are adequate and work as designed. This is key in managing risks associated with the confidentiality, integrity, and availability of healthcare and other sensitive data processed within the app.

This process should be more than just a checklist of controls for your developers. Risk analysis and ongoing risk management should always focus on the risk and its potential impact on PHI and your operational resilience.

Clearwater is the leading provider of Enterprise Cyber Risk Management and HIPAA compliance software and consulting services for the healthcare industry. Our solutions enable organizations to gain enterprise-wide visibility into cybersecurity risks and more effectively prioritize and manage them, ensuring compliance with industry regulations. Clearwater's suite of IRM|Pro® software products and consulting services help healthcare organizations to avoid preventable breaches, protect patients and their data, and meet OCR's expectations, while optimizing cybersecurity investments. More than 400 healthcare organizations, including 64 of the nation's largest health systems and a large universe of business associates that serve the industry, trust Clearwater to meet their information security needs.

Have questions regarding this white paper? Engage with Clearwater for a specific discussion about your organization's approach.

- ClearwaterSecurity.com/Contact