Updates
December 01, 2020

# DHHS Updates Resources for Mobile Health App Developers

The COVID-19 pandemic and the resulting need for patient access to remote healthcare, as well as the development of contact-tracing apps, have spotlighted the importance of health-focused mobile applications (mHealth apps). The mHealth app industry is booming, with a market size projected to grow from approximately $11 billion in 2018 to almost $60 billion by 2026. COVID-19 has almost certainly accelerated this trend.

On September 1, 2020, the U.S. Department of Health & Human Services' Office for Civil Rights (OCR) updated its Health App Developer Portal, renaming it Resources for Mobile Health Apps Developers. The revised resource page addresses issues regarding the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as it relates to mHealth apps, cloud computing, and related application program interfaces (APIs).

Healthcare stakeholders, including providers and electronic health record (EHR) vendors, will need to understand how the updated resource page applies to them as well as to the electronic protected health information (ePHI) they collect, use, share, and store.

### The OCR's Role in Regulating mHealth Apps

The OCR directs various initiatives to develop and regulate the burgeoning industry of mHealth apps. To cite one example, the Centers for Medicare & Medicaid Services (CMS) has been implementing a plan to help patients more easily download their health information to their smartphones. In fulfillment of this plan, on March 9, 2020, CMS issued the Interoperability and Patient Access Final Rule, which lays out policies to foster greater interoperability and data-exchange capabilities throughout the healthcare system. The final rule requires implementation of APIs to allow patients to easily access and transfer their information to their smartphones and designated mHealth apps. It applies to healthcare providers; Medicaid, Medicare, and Children's Health Insurance Program (CHIP) programs; and health plans on federally facilitated exchanges that qualify under the Affordable Care Act (ACA).

Other examples of OCR's initiatives in this area include its 2016 guidance, addressing how HIPAA applies to health information a patient creates, manages, or organizes via a patient-focused mHealth app and when an mHealth app developer may be required to comply with the HIPAA Rules.

### OCR Resources for Mobile Health Apps Developers

The OCR is also in charge of applying and enforcing HIPAA and its implementing regulations in relation to mHealth apps and related technologies. The resource page is one central mechanism the OCR uses to fulfill this responsibility. We note that it is possible the incoming Biden administration may revise the Resources for Mobile Health Apps Developers page after they take office in January 2021, but the content will need to remain broadly consistent with the final rule unless officially changed (though the new administration could choose to waive certain requirements without a formal rule change).

At a high level, the resource page does the following:

- Provides links addressing the intersection of health information technology and HIPAA privacy and security requirements
- Assists health IT professionals with understanding how the HIPAA regulations, including the HIPAA Right of Access, apply to developing mHealth apps
- Supports entities and business associates in understanding their compliance obligations regarding HIPAA and cloud-computing technologies

We highlight two key developments announced by OCR on the updated resource page, while noting that the page also contains new guidance on a variety of other topics not covered here.

First, the updated resource page clarifies how mHealth apps should be addressed in the relationships between "covered entities" (healthcare providers, health plans, or healthcare clearinghouses) and their "business associates" (persons or entities that create, receive, maintain, or transmit ePHI on behalf of, or for the benefit of, such covered entity). In particular, the new page addressing the access right, health apps, and APIs discusses these relationships in the following two contexts: (1) when an mHealth app developer itself is subject to HIPAA; and (2) when HIPAA applies to ePHI transmitted to an mHealth app.

The resource page clarifies that if the mHealth app is creating, receiving, maintaining, or transmitting ePHI on behalf of or for the benefit of a covered entity, HIPAA will apply directly to the mHealth app as it is acting as a business associate to the covered entity. However, if a patient directs a covered entity to transmit, or the patient directly transmits, their ePHI to an mHealth app, the mHealth app is not performing services on behalf of the covered entity and is, therefore, not a business associate to which HIPAA would apply.

The same analysis applies through multiple levels. An mHealth app developer can be a sub-business associate to a business associate if the developer creates, receives, maintains, or transmits ePHI on behalf of such business associate. As an example, if a covered entity's EHR system developer is a business associate of such covered entity and if an mHealth app creates, receives, maintains, or transmits ePHI on behalf of the EHR system developer, then the mHealth app is a sub-business associate. In this case, the EHR system developer must bind the mHealth app to a sub-business associate agreement with terms equivalent to those in the business associate agreement between the EHR system developer and the covered entity.

Further, the resource page's new guidance states that a covered entity must fulfill an individual's right of access under HIPAA and disclose the individual's ePHI to an app designated by the individual, even if the covered entity has concerns about the security of the app or how the app will use the individual's ePHI.

Second, the updated resource page also provides new guidance for how covered entities and business associates may compliantly leverage cloud service providers (CSPs). The CSP guidance intersects with the mHealth app guidance, as mHealth apps are often hosted on the cloud. If the CSP creates, receives, maintains, or transmits ePHI on behalf of (or for the benefit of) a covered entity or another business associate, the CSP is a business associate under HIPAA. Notably, the resource page clarifies that a CSP that meets the definition of a business associate must comply with all provisions of the HIPAA rules regardless of whether it is a business associate directly to a covered entity or it is acting in the role of a sub-business associate (i.e., providing services to a covered entity's business associate).

In summary, it is critical for the healthcare industry to understand the criteria for when and how HIPAA applies to mHealth apps and cloud computing, as well as the relationships between the various entities involved in transmitting ePHI. The OCR's updated resource page provides important new guidance in these areas. Providers, insurers, and healthcare technology companies should review these developments to understand their compliance obligations and potential vulnerabilities when their specific operations and circumstances involve mHealth apps and related technologies.

## Explore more in

Technology Transactions & Privacy Law  Privacy & Security  Healthcare

**Related insights**

Update

### Ninth Circuit Rejects Mass-Arbitration Rules, Backs California Class Actions

Update

### CFPB Finalizes Proposed Open Banking Rule on Personal Financial Data Rights