Health App Use Scenarios & HIPAA

These scenarios address two questions under the Health Insurance Portability and Accountability Act (HIPAA):

1. How does HIPAA apply to health information that a patient creates, manages or organizes through the use of a health app?
2. When might an app developer need to comply with the HIPAA Rules?

The answers to these questions are fact and circumstance specific. Each scenario below is based on a specific set of facts. Please keep this in mind as you review a scenario and apply it to your own circumstances. Change in a scenario may change the analysis and, as a result, change the determination of whether the app developer is required to comply with HIPAA. We hope this will help you identify the particular aspects to explore in your own analysis.

***Background*:**

Only health plans, health care clearinghouses and most health care providers are *covered entities* under HIPAA. If you work for one of these entities, and as part of your job you are creating an app that involves the use or disclosure of identifiable health information, the entity (and you, as a member of its workforce) must protect that information in compliance with the HIPAA Rules. For extensive information on the requirements of the HIPAA rules and how to comply with them, please see http://www.hhs.gov/hipaa/index.html

However, even if you are not a covered entity, you may be a *business associate* if you are creating or offering the app on behalf of a covered entity (or one of the covered entity's contractors) – and in that case you are required to comply with certain provisions of the HIPAA Rules. In general, a business associate is a person [or entity] who creates, receives, maintains or transmits protected health information (PHI) on behalf of a covered entity or another business associate. PHI is defined in the HIPAA regulations, and, in general, is identifiable health information. So, most vendors or contractors (including subcontractors) that provide services to or perform functions for covered entities that involve access to PHI are business associates. For example, a company that is given access to PHI by a covered entity to provide and manage a personal health record or patient portal offered by the covered entity to its patients or enrollees is a business associate.

Note that the scenarios below address the application of HIPAA to the app developer. In all cases in which a covered entity is transmitting PHI, either itself or using a business associate, it must apply reasonable safeguards to protect the information and nothing in the analyses below relieves covered entities (e.g., providers) of their own, independent obligation to comply with HIPAA.

Scenario	*Based on the Facts Presented in the Scenario, Is App Developer a HIPAA Business Associate?*
Consumer downloads a health app to her smartphone. She populates it with her own information. For example, the consumer inputs blood glucose levels and blood pressure readings she obtained herself using home health equipment.	*No. Developer is not creating, receiving, maintaining or transmitting protected health information (PHI) on behalf of a covered entity or another business associate. The consumer is using the developer's app to help her manage and organize her information without any involvement of her health care providers.*
Consumer downloads a health app to her smartphone that is designed to help her manage a chronic condition. She downloads data from her doctor's EHR through a patient portal, onto her computer and then uploads it into the app. She also adds her own information to the app.	*No. Developer is not creating, receiving, maintaining or transmitting protected health information (PHI) on behalf of a covered entity or another business associate. Instead, the consumer obtains health information from her provider, combines it with health information she inputs, and uses the app to organize and manage that information for her own purposes. There is no indication the provider or a business associate of the provider hired the app developer to provide or facilitate this service.*
Doctor counsels patient that his BMI is too high, and recommends a particular app that tracks diet, exercise, and weight. Consumer downloads app to his smartphone and uses it to send a summary report to his doctor before his next appointment.	*No. Developer is not creating, receiving, maintaining or transmitting protected health information (PHI) on behalf of a covered entity or another business associate. The doctor's recommendation implies her trust in the app, but there is no indication that the doctor hired the app developer to provide services to patients involving the handling of PHI. The consumer's use of an app to transmit data to a covered entity does not by itself make the app developer a BA of the covered entity.*
Consumer downloads a health app to her smartphone that is designed to help her manage a chronic condition. Health care provider and app developer have entered into an interoperability arrangement at the consumer's request that facilitates secure exchange of consumer information between the provider EHR and the app. The consumer populates information on the app and directs the app to transmit the information to the provider's EHR. The consumer is able to access test results from the provider through the app.	No. Developer is not creating, receiving, maintaining or transmitting protected health information (PHI) on behalf of a covered entity or another business associate. The interoperability arrangement alone does not create a BA relationship because the arrangement exists to facilitate access initiated by the consumer. The app developer is providing a service to the consumer, at the consumer's request and on her behalf. The app developer is transmitting data on behalf of the consumer to and from the provider; this activity does not create a BA relationship with the covered entity.

Scenario	*Based on the Facts Presented in the Scenario, Is App Developer a HIPAA Business Associate?*
At direction of her provider, patient downloads a health app to her smart phone. Provider has contracted with app developer for patient management services, including remote patient health counseling, monitoring of patients' food and exercise, patient messaging, EHR integration and application interfaces. Information the patient inputs is automatically incorporated into provider EHR.	*Yes, the developer is a business associate of the provider, because it is creating, receiving, maintaining and transmitting protected health information (PHI) on behalf of a covered entity. In this case, the provider contracts with the app developer for patient management services that involve creating, receiving, maintaining and transmitting PHI, and the app is a means for providing those services.*
Consumer downloads to her smart phone a mobile PHR app offered by her health plan that offers users in its network the ability to request, download and store health plan records and check the status of claims and coverage decisions. The app also contains the plan's wellness tools for members, so they can track their progress in improving their health. Health plan analyzes health information and data about app usage to understand effectiveness of its health and wellness offerings. App developer also offers a separate, direct-to-consumer version of the app that consumers can use to store, manage, and organize their health records, to improve their health habits and to send health information to providers.	*Yes, with respect to the app offered by the health plan, and no, when offering the direct-to-consumer app. Developer is a business associate of the health plan, because it is creating, receiving, maintaining or transmitting protected health information (PHI) on behalf of a covered entity. Developer must comply with applicable HIPAA Rules requirements with respect to the PHI involved in its work on behalf of the health plan. But its "direct-to-consumer" product is not provided on behalf of a covered entity or other business associate, and developer activities with respect to that product are not subject to the HIPAA Rules. Therefore, as long as the developer keeps the health information attached to these two versions of the app separate, so that information from the direct-to-consumer version is not part of the product offering to the covered entity health plan, the developer does not need to apply HIPAA protections to the consumer information obtained through the "direct-to- consumer" app.*

Key Questions

If you are an app vendor, and you are not already a covered entity, you should consider the following questions in determining whether or not you may be a business associate – i.e., an entity that creates, receives, maintains or transmits protected health information (PHI) on behalf of a covered entity or business associate:

- Does your health app create, receive, maintain, or transmit identifiable information?
- Who are your clients? How are you funded?
  - Are your clients covered entities? e.g.,
    - hospitals, doctor's offices, clinics, pharmacies, or other health care providers who conduct electronic transactions;
    - health insurance issuers; health or wellness program related to a health plan offered by an employer
  - Were you hired by, or are you paid for your service or product by, a covered entity? Or another business contracted to a covered entity?
  - Does a covered entity (or a business associate acting on its behalf) direct you to create, receive, maintain or disclose information related to a patient or health plan member?

If you are only offering services directly to and collecting information for or on behalf of consumers, and not on behalf a provider, health plan or health care clearinghouse, you are not likely to be subject to HIPAA as either a covered entity or business associate.

- Is your app independently selected by a consumer?
- Does the consumer control all decisions about whether to transmit her data to a third party, such as to her health care provider or health plan?
- Do you have no relationship with that third party entity (other than an interoperability relationship)?

If you make the determination that you are not a covered entity, or your business model does not include acting as a business associate, protecting the privacy and security of consumers' data is still important. You may find these resources helpful.

- Mobile App Developers: Start with Security, https://www.ftc.gov/tips-advice/business-center/guidance/mobile-app-developers-start-security
- Marketing Your Mobile App: Get it Right from the Start, https://www.ftc.gov/tips-advice/business-center/guidance/marketing-your-mobile-app-get-it-right-start