U.S. Department of Health and Human Services Office of Civil Rights
FAQs – Right to Access and HIT (updated 4/18/2019)

Does a HIPAA covered entity that fulfills an individual's request to transmit electronic protected health information (ePHI) to an application or other software (collectively "app") bear liability under the HIPAA Privacy, Security, or Breach Notification Rules (HIPAA Rules) for the app's use or disclosure of the health information it received?

The answer depends on the relationship between the covered entity and the app. Once health information is received from a covered entity, at the individual's direction, by an app that is neither a covered entity nor a business associate under HIPAA, the information is no longer subject to the protections of the HIPAA Rules. If the individual's app – chosen by an individual to receive the individual's requested ePHI – was not provided by or on behalf of the covered entity (and, thus, does not create, receive, transmit, or maintain ePHI on its behalf), the covered entity would not be liable under the HIPAA Rules for any subsequent use or disclosure of the requested ePHI received by the app. For example, the covered entity would have no HIPAA responsibilities or liability if such an app that the individual designated to receive their ePHI later experiences a breach.

If, on the other hand, the app was developed for, or provided by or on behalf of the covered entity – and, thus, creates, receives, maintains, or transmits ePHI on behalf of the covered entity – the covered entity could be liable under the HIPAA Rules for a subsequent impermissible disclosure because of the business associate relationship between the covered entity and the app developer. For example, if the individual selects an app that the covered health care provider uses to provide services to individuals involving ePHI, the health care provider may be subject to liability under the HIPAA Rules if the app impermissibly discloses the ePHI received.

What liability does a covered entity face if it fulfills an individual's request to send their ePHI using an unsecure method to an app?

Under the individual right of access, an individual may request a covered entity to direct their ePHI to a third-party app in an unsecure manner or through an unsecure channel. See 45 CFR 164.524(a)(1), (c)(2)(ii), (c)(3)(ii). For instance, an individual may request that their unencrypted ePHI be transmitted to an app as a matter of convenience. In such a circumstance, the covered entity would not be responsible for unauthorized access to the individual's ePHI while in transmission to the app. With respect to such apps, the covered entity may want to consider informing the individual of the potential risks involved the first time that the individual makes the request.

Where an individual directs a covered entity to send ePHI to a designated app, does a covered entity's electronic health record (EHR) system developer bear HIPAA liability after completing the transmission of ePHI to the app on behalf of the covered entity?

The answer depends on the relationship, if any, between the covered entity, the EHR system developer, and the app chosen by the individual to receive the individual's ePHI. A business associate relationship exists if an entity creates, receives, maintains, or transmits ePHI on behalf of a covered entity (directly or through another business associate) to carry out the covered functions of the covered entity. A business associate relationship exists between an EHR system developer and a covered entity. If the EHR system developer does not own the app, or if it owns the app but does not provide the app to, through, or on behalf of, the covered entity – e.g., if it creates the app and makes it available in an app store as part of a different line of business (and not as part of its business associate relationship with any covered entity)

– the EHR system developer would not be liable under the HIPAA Rules for any subsequent use or disclosure of the requested ePHI received by the app.

If the EHR system developer owns the app or has a business associate relationship with the app developer, and provides the app to, through, or on behalf of, the covered entity (directly or through another business associate), then the EHR system developer could potentially face HIPAA liability (as a business associate of a HIPAA covered entity) for any impermissible uses and disclosures of the health information received by the app. For example, if an EHR system developer contracts with the app developer to create the app on behalf of a covered entity and the individual later identifies that app to receive ePHI, then the EHR system developer could be subject to HIPAA liability if the app impermissibly uses or discloses the ePHI received.

Can a covered entity refuse to disclose ePHI to an app chosen by an individual because of concerns about how the app will use or disclose the ePHI it receives?

No. The HIPAA Privacy Rule generally prohibits a covered entity from refusing to disclose ePHI to a third-party app designated by the individual if the ePHI is readily producible in the form and format used by the app. See 45 CFR 164.524(a)(1), (c)(2)(ii), (c)(3)(ii). The HIPAA Rules do not impose any restrictions on how an individual or the individual's designee, such as an app, may use the health information that has been disclosed pursuant to the individual's right of access. For instance, a covered entity is not permitted to deny an individual's right of access to their ePHI where the individual directs the information to a third-party app because the app will share the individual's ePHI for research or because the app does not encrypt the individual's data when at rest. In addition, as discussed in Question 1 above, the HIPAA Rules do not apply to entities that do not meet the definition of a HIPAA covered entity or business associate.

Does HIPAA require a covered entity or its EHR system developer to enter into a business associate agreement with an app designated by the individual in order to transmit ePHI to the app?

It depends on the relationship between the app developer, and the covered entity and/or its EHR system developer. A business associate is a person or entity who creates, receives, maintains or transmits PHI on behalf of (or for the benefit of) a covered entity (directly or through another business associate) to carry out covered functions of the covered entity. An app's facilitation of access to the individual's ePHI at the individual's request alone does not create a business associate relationship. Such facilitation may include API terms of use agreed to by the third-party app (i.e., interoperability arrangements).

HIPAA does not require a covered entity or its business associate (e.g., EHR system developer) to enter into a business associate agreement with an app developer that does not create, receive, maintain, or transmit ePHI on behalf of or for the benefit of the covered entity (whether directly or through another business associate).

However if the app was developed to create, receive, maintain, or transmit ePHI on behalf of the covered entity, or was provided by or on behalf of the covered entity (directly or through its EHR system developer, acting as the covered entity's business associate), then a business associate agreement would be required.

More information about apps, business associates, and HIPAA is available at https://hipaaqsportal.hhs.gov