HIPAA liability depends upon the relationship between the covered entity and the app

HHS OCR recently released five FAQs addressing the liability of covered entities or business associates under HIPAA privacy, security, or breach notification rules (HIPAA rules) for impermissible disclosure of electronic protected health information (ePHI) by a health app developer.

These FAQs state that the key to HIPAA liability is the relationship between the covered entity and the app. That is, once the app receives health information from the covered entity, and as directed by an individual, the health information is longer subject to HIPAA rules. The individual’s app was not provided by or on behalf of the covered entity (and thus, does not create, receive, transmit, or maintain ePHI on its behalf) and in this circumstance the covered entity would not be liable for any subsequent impermissible disclosure of the ePHI. However, if the app was developed for, or provided by or on behalf of the covered entity and creates, receives, maintains, or transmits ePHI on behalf of the covered entity, it would be liable under the HIPAA rules for any subsequent impermissible disclosure because the app developer and the covered entity are in a business associate relationship.

Under HIPAA an individual has a right to request a covered entity to direct their ePHI to a third-party app in an unsecured manner or through an unsecure channel. In such case the covered entity would not be responsible for unauthorized access to ePHI during such transmission to the app. OCR recommends informing the individual of any potential risks when the individual first makes the request.

Again, the relationship between the covered entity, the electronic health record (EHR) system developer and the app is key to liability under HIPAA where an individual directs a covered entity to send ePHI to a designated app. The EHR is not liable under the HIPPA rules for subsequent violations, if it does not own the app or it does own the app but does not provide it to, through, or on behalf of the covered entity. However, the EHR may potentially face HIPAA liability if it 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.

OCR states that a covered entity cannot refuse to disclose ePHI to an app based on concerns about how the app will use or disclose ePHI. Nor can the covered entity impose restrictions on the individual or the app. The HIPAA Rules do not apply to entities that do not meet the definition of a HIPAA covered entity or business associate. Furthermore, HIPAA does not require a covered entity or its business associate (e.g., EHR) to enter into a business associate agreement with the app developer unless 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 EHR acting as the covered entity’s business associate).

*https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access-right-health-apps-apis/index.html