THIRD PARTY APPS – WHAT YOU SHOULD KNOW

When a member shares protected health information with a third-party app or requests Brand New Day (a Bright HealthCare Company) to share their health data with an app, Brand New Day (a Bright HealthCare Company) is not liable for any subsequent use or disclosure of the data as long as the app developer is not a business associate of Brand New Day (a Bright HealthCare Company). Therefore, Brand New Day (a Bright HealthCare Company) would have no HIPAA responsibilities or liability if an app that a member designated to receive their protected health information later experienced a breach.

Further, once a member downloads their data, they are responsible for that data. Once data is downloaded to an app secondary use and disclosure should be considered. Liability of stewardship of the data ends once the member downloads it, unless the app was developed for, or provided by, or on behalf of Brand New Day (a Bright HealthCare Company) and thus, creates, receives, maintains, or transmits electronic protected health information.

❖ IMPORTANT ITEMS MEMBERS SHOULD CONSIDER BEFORE AUTHORIZING A THIRD-PARTY APP TO RETRIEVE THEIR HEALTHCARE DATA

It is important for members to take an active role in protecting your health information. The below serves as a guide for members to know what to look for when choosing an app.

- Members should look for an easy-to-read privacy policy that clearly explains how the app will use their data.
- What health data will this app collect? Will this app collect non-health data from my device, such as my location?
- Will my data be stored in a de-identified or anonymized form?
    - De-identification of data is where identifiers are removed from a data set which results in data that is no longer considered PHI for purposes of HIPAA. De-identification is a process which can be reversed.
    - Anonymization is the act of permanently and completely removing personal identifiers from data. Anonymized data is data that can no longer be associated with an individual in any manner. Once this data is stripped of personally identifying elements, those elements can never be re-associated with the data or the underlying individual.
- How will this app use my data?
- Will this app disclose my data to third parties?
    - Will this app sell my data for any reason, such as advertising or research?
    - Will this app sell my data for any reason, such as advertising or research?
- How can I limit this app's use and disclosure of my data?
- What security measures does this app use to protect my data?
- What impact could sharing my data with this app have on others, such as my family members?
- How can I access my data and correct inaccuracies in data retrieved by this app?
- Does this app have a process for collecting and responding to user complaints?
- If I no longer want to use this app, or if I no longer want this app to have access to my health information, how do I terminate the app's access to my data?
    - What is the app's policy for deleting my data once I terminate access? Do I have to do more than just delete the app from my device?
- How does this app inform users of changes that could affect its privacy practices?

If the app's privacy policy does not clearly answer these questions, members should reconsider using the app to access their health information. Health information is very sensitive information, and members should be careful to choose apps with strong privacy and security standards to protect it.

What should a patient consider if they are part of an enrollment group?
Some members, particularly members who are covered by Qualified Health Plans (QHPs) on the Federally facilitated Exchanges (FFEs), may be part of an enrollment group where they share the same health plan as multiple members of their tax household. Often, the primary policy holder and other members, can access information for all members of an enrollment group unless a specific request is made to restrict access to member data. Members should be informed about how their data will be accessed and used if they are part of an enrollment group based on the enrollment group policies of their specific health plan in their specific state. Members who share a tax household but who do not want to share an enrollment group have the option of enrolling individual household members into separate enrollment groups, even while applying for Exchange coverage and financial assistance on the same application; however, this may result in higher premiums for the household and some members, (i.e. dependent minors, may not be able to enroll in all QHPs in a service area if enrolling in their own enrollment group) and in higher total out-of-pocket expenses if each member has to meet a separate annual limitation on cost sharing (i.e., Maximum Out-of-Pocket (MOOP)).

What are a patient's rights under the Health Insurance Portability and Accountability Act (HIPAA) and who must follow HIPAA?
The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) enforces the HIPAA Privacy, Security, and Breach Notification Rules, and the Patient Safety Act and Rule. The Privacy Rule, a Federal law, gives you rights over your health information and sets rules and limits on who can look at and receive your health information. The Privacy Rule applies to all forms of individuals' protected health information, whether electronic, written, or oral. The Security Rule is a Federal law that requires security for health information in electronic form.

❖ ACCESS RIGHTS, APPS, and APIs FAQs

The below provides responses to frequently asked questions specific to Apps, APIs, and Access Rights:

1. Q: 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?

A: 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.

2. Q: 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?
A: 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.
3. Q: 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?
A: 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.
4. Q: 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?
A: 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.
5. Q: 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?
A: 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.

❖ WHICH TYPES OF ORGANZAITIONS OR INDIVIDUALS ARE LIKELY TO BE HIPAA COVERED ENTITIES

Those who must comply with HIPAA are often called HIPAA-covered entities. HIPAA-covered entities include health plans, clearinghouses, and certain health care providers. Most entities which are not addressed below are not regarded as covered entities.

Health Plans
For HIPAA purposes, health plans include:

- Health insurance companies
- HMOs, or health maintenance organizations
- Employer-sponsored health plans
- Government programs that pay for health care, like Medicare, Medicaid, and military and veterans' health programs

Clearinghouses
Clearinghouses include organizations that process nonstandard health information to conform to standards for data content or format, or vice versa, on behalf of other organizations.

Providers
Providers who submit HIPAA transactions, like claims, electronically are covered. These providers include, but are not limited to:

- Doctors
- Clinics
- Psychologists
- Dentists
- Chiropractors
- Nursing homes
- Pharmacies

About Business Associates
If a covered entity engages a business associate to help carry out its health care activities and functions, the covered entity must have a written business associate contract or other arrangement with the business associate that:

- Establishes specifically what the business associate has been engaged to do
- Requires the business associate to comply with HIPAA

Examples of business associates include:

- Third-party administrator that assists a health plan with claims processing
- Consultant that performs utilization reviews for a hospital
- Health care clearinghouse that translates a claim from a nonstandard format into a standard transaction on behalf of a health care provider, and forwards the processed transaction to a payer
- Independent medical transcriptionist that provides transcription services to a physician

Also, a covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity.

❖ HOW TO FILE A COMPLAINT

Complaint Process - OCR
If you believe that a HIPAA-covered entity or its business associate violated your (or someone else's) health information privacy rights or committed another violation of the Privacy, Security, or Breach Notification Rules, you may file a complaint with the Office for Civil Rights (OCR).

- **File a Complaint Online**
  - File your complaint electronically via the OCR Complaint Portal:
    U.S. Department of Health & Human Services - Office for Civil Rights (hhs.gov)

- **File a Complaint in Writing**
  - Open and fill out the Health Information Privacy Complaint Form Package - PDF in PDF format. You will need Adobe Reader software to fill out the complaint and consent forms. You may either:
    - *Print and mail the completed complaint and consent forms to:*
      Centralized Case Management Operations
      U.S. Department of Health and Human Services
      200 Independence Avenue, S.W.
      Room 509F HHH Bldg.
      Washington, D.C. 20201
    - *Email the completed complaint and consent forms to OCRComplaint@hhs.gov (Please note that communication by unencrypted email presents a risk that personally identifiable information contained in such an email, may be intercepted by unauthorized third parties)*

- **File a Complaint Without Using the Health Information Privacy Complaint Package**
  - If you prefer, you may submit a written complaint in your own format by either:
    - Print and mail the completed complaint and consent forms to:
      Centralized Case Management Operations
      U.S. Department of Health and Human Services
      200 Independence Avenue, S.W.
      Room 509F HHH Bldg.
      Washington, D.C. 20201
  - Email to OCRComplaint@hhs.gov
    - *Be sure to include:*

    Your name; Full address; Telephone numbers (include area code); E-mail address (if available); Name, full address and telephone number of the person, agency, or organization you believe violated your (or someone else's) health information privacy rights or committed another violation of the Privacy or Security Rule; Brief description of what happened. How, why, and when do you believe your (or someone else's) health information privacy rights were violated; or how the Privacy or Security Rule otherwise was violated; Any other relevant information; Your signature and date of complaint;

    If you are filing a complaint on someone's behalf, also provide the name of the person on whose behalf you are filing.

    - *You may also include:*

If you need special accommodations for us to communicate with you about this complaint;
Contact information for someone who can help us reach you if we cannot reach you directly;
If you have filed your complaint somewhere else and where you've filed.

Please note, that Not all entities are required to comply with the Privacy and Security Rules. OCR can only investigate the **covered entities** that must comply with these rules. **Covered entities** include most:

- Doctors
- Clinics
- Hospitals
- Psychologists
- Chiropractors
- Nursing Homes
- Pharmacies
- Dentists
- Health Insurance Companies
- Company Health Plans
- Medicare, Medicaid, and other government programs that pay for health care

Complaint Process - FTC

If you believe you have been subjected to fraud, scams or bad business practices, please visit the below link to report such instances:

- https://www.ftccomplaintassistant.gov/#crnt&panel1-1

THIRD PARTY APP DEVELOPERS

Brand New Day (a Bright HealthCare Company) Developer Portal Link

Link to Developer Portal