

Choosing a Third Party to Access and Making Your Health Information Available

In accordance with federal law, we are required to provide our current members enrolled in Medicare, Medicaid, or plans purchased through the HealthCare Marketplace with access to a subset of personal information through apps they may choose to share their personal data with. Additionally, we make this data available to other health plans or payers of our current member's choice.

Both of these services are provided through an interface maintained by Ascension. The information made available includes, but is not limited to:

- Demographic information such as name, address, date of birth
- Claims information such as amounts paid for services
- Clinical information, such as visit information, diagnoses, treatments, medications, disorders, and other information considered sensitive

If approved by you, apps made by third parties, health plans, and insurance companies can connect to this interface and retrieve your data.

Please note, once consent is given to an app, health plan or payer, Ascension is no longer responsible for securing and/or protecting data once it leaves our network. It is up to you to ensure that they have done the appropriate research to understand how that third party collects, stores, and protects data.

If you have any questions about the data, you should contact the original source of the data directly. If you have any specific health questions about your diagnosis, you should contact the provider who provided this information.

It is important for our members to take an active role in protecting their health information. You should look for an easy-to-read privacy policy that clearly explains how the app will use your data. If an app does not have a privacy policy, we would advise you to not use this app.

Here are some things you may wish to consider:

- 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?
- 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 share my data for any reason? If so, with whom? For what purpose?
- 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?

Apps, Member's Rights, and Privacy Enforcement

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.

You can find more information about your rights under HIPAA and who is obligated to follow HIPAA here:

<https://www.hhs.gov/hipaa/for-individuals/guidance-materials-forconsumers/index.html>

Additionally, you may want to review the HIPAA FAQ for individuals here:

<https://www.hhs.gov/hipaa/for-individuals/faq/index.html>

Most third-party apps will not be covered by HIPAA. Most third-party apps will instead fall under the jurisdiction of the Federal Trade Commission (FTC) and the protections provided by the FTC Act.

The FTC provides information about mobile app privacy and security for consumers here:

<https://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps>

You can make a complaint to OCR or FTC about an app. You can do this if you believe an app has used, disclosed, or sold your Personal Information inappropriately or in a way that is not consistent with its privacy policy.

To learn more about filing a complaint with OCR related to HIPAA requirements, visit:

<https://www.hhs.gov/hipaa/filing-a-complaint/index.html>

You may file a complaint with OCR using the OCR compliant portal:

<https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf>

You may file a complaint with the FTC using the FTC complaint assistant here:

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

If you have questions or would like to file a plan-specific complaint, please contact customer service at the phone number on your ID card.