

# Health Plan Patient Access API

## User Education

We are required to provide you with access to detailed information about your health history through a “Patient Access API.” You may access this information by downloading an App on your smart phone, tablet, computer or other similar device. The information available through the Patient Access API includes information we collect about you while you have been enrolled in your health plan. The information includes the following information while we maintain it in our records:

- Claims and “encounter” data<sup>1</sup> concerning your interactions with health care providers; and
- Clinical data that we collect in the process of providing case management, care coordination, or other services to you.

**The information we will disclose may include information about treatment for Substance Use Disorders, mental health treatment, HIV status, or other sensitive information.**

We want you to know the App you choose will have access to *all* of your information. The App is *not* subject to the HIPAA Rules, which generally protect your health information. Instead, the App’s privacy policy describes self-imposed limitations on how the App will use, disclose, and (possibly) sell information about you. It is important for you to know once we send your data to the App, we no longer control how the App uses or shares your information. If you decide to access your information through the Patient Access API, you should carefully review the privacy policy of any App you are considering using to ensure you are comfortable with what the App will do with your information.

Things you may wish to consider when selecting an App:

- Will this App *sell* my data for any reason?
- Will this App *disclose* my data to third parties for purposes such as research or advertising?
- How will this App *use* my data? For what purposes?
- Will the App allow me to limit how it uses, discloses, or sells my data?
- If I no longer want to use this App, or if I no longer want this App to have access to my health information, can I terminate the App’s access to my data? If so, how difficult will it be to terminate access?
- 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 in its privacy practices?
- Will the App collect non-health data from my device, such as my location?

---

<sup>1</sup> Some providers send us Encounter data about your health care, such as information about your office visits, in cases where they do not send us a claim.

- 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?
- Will the App permit me to access my data and correct inaccuracies? (Note that correcting inaccuracies in data collected by the App will not affect inaccuracies in the source of the data.)
- Does the App have a process for collecting and responding to user complaints?

If the App's privacy policy does not satisfactorily answer these questions, you may wish to reconsider using the App to access your health information. Your health information may include very sensitive information. You should therefore be careful to choose an App with strong privacy and security standards to protect it. If the App does not have a privacy policy, you may want to consider not using the App.

### **Covered Entities and HIPAA Enforcement**

The U.S. Department of Health and Human Services' Office for Civil Rights (OCR) enforces the HIPAA Privacy, Security, and Breach Notification Rules. We are subject to HIPAA as are most health care providers, such as hospitals, doctors, clinics, and dentists. 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/index.html>. 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 also file a complaint with us by contacting the Member Services phone number on your ID card.

### **Apps and Privacy Enforcement**

An App generally **will not** be subject to HIPAA. An App that publishes a privacy notice is required to comply with the terms of its notice, but generally is not subject to other privacy laws. The Federal Trade Commission Act protects against deceptive acts (such as an App that discloses personal data in violation of its privacy notice). An App that violates the terms of its privacy notice is subject to the jurisdiction of the Federal Trade Commission (FTC). The FTC provides information about mobile App privacy and security for consumers here: <https://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps>.

If you believe an App inappropriately used, disclosed, or sold your information, you should contact the FTC. You may file a complaint with the FTC using the FTC complaint assistant: <https://www.ftccomplaintassistant.gov/#crnt&panel1-1>. You may also wish to consider deleting the App.