BlueCross BlueShield of Oklahoma

PLEASE READ

IMPORTANT MEMBER INFORMATION

Choosing an Application to Access Your Health Information

Making Your Health Information Available to Another Health Plan or Payer

This notice provides information about the privacy and security of the health information that Blue Cross and Blue Shield of Oklahoma (BCBSOK) (the "Plan", "we", "us") maintains about you. This information is called your Personal Information. When your Personal Information is made available to you through a third-party application ("App") or to a health plan or payer of your choice, it is important for you to know that this information is at risk.

Federal law requires us to provide current members who have Medicare, Medicaid and plans purchased through the Health Care Marketplace with access to certain Personal Information through Apps of their choice (the Patient Access Process). The federal law also requires that members can make their Personal Information available to another health plan or payer of the member's choice (the Payer to Payer Data Exchange). We will do this by allowing Apps or other health plans or payers to connect to an application programming interface ("API") we maintain.

The Personal Information that may be available through the API includes:

- Your name, address, date of birth, amounts paid to providers, claims information, as well as other Personal Information, and
- Your clinical information, which may include diagnoses and medical treatments, including treatment for substance use disorders, mental health treatment, HIV status, or other sensitive Personal Information.

This information is only for services on or after January 1, 2016.

Third-party App developers and other health plans or payers can connect to our API. This will allow access to your Personal Information. This means you, the other heath plan or payer, and App developers can see your information. As a current Plan member, or someone who has authorization to a Plan member's Personal Information, you may decide to download an App to your smart phone, tablet, computer or other similar device. **This decision is up to you**.

Once your Personal Information is released to the App or to another health plan or payer of your choice, the Plan is no longer responsible for securing or protecting the information. If you decide to access your Personal Information through an App, be sure you are comfortable with what the App will do with your Personal Information and how the App will protect your information.

If you choose to use an App to access your Personal Information through the Patient Access Process or make your Personal Information available through the Payer to Payer Data Exchange, you will be required to sign a Member Consent. This will authorize us to complete your request and make your Personal Information available. If you do not sign the Member Consent, we cannot make the Personal Information available.

In some cases we are not the original source of the Personal Information that we maintain. The original source may include your provider (hospital, doctor, or medical clinic). In those cases if you have any health questions about your medical diagnosis or treatment you should contact your provider.

Choosing a Patient Access Process App with Strong Privacy and Security Standards

It is important to understand that if you download an App for the Patient Access Process, the App you select will have access to all of your Personal Information that the Plan maintains. This includes your sensitive Personal Information as described above.

You should carefully review the App's privacy policy. It should describe how the App will protect, use, disclose, and possibly sell your Personal Information. If an App does not have a privacy policy, we do not recommend that members choose the App for connection with our API.

Here are some things you may wish to consider when selecting a Patient Access Process App:

- Will this App ***sell*** my data for any reason, such as research or advertising?
- Will this App ***share*** my data with third parties? If so, with whom? For what purpose?
- How will this App ***use*** my data?
- 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 Personal 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 will this App inform me of changes in its privacy practices?
- Will the App collect non-health data from my device, such as my location?
- 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 allow me to correct any data that is not accurate?
- Does the App have a process for collecting and responding to user complaints?

Be careful to choose an App with strong privacy and security standards. If you are not satisfied with the answers an App's privacy policy has for these questions, you may not want to use the App.

Apps, Member's Rights, and Privacy Enforcement

The U.S. Department of Health and Human Services' Office for Civil Rights (OCR) enforces the HIPAA Privacy, Security, and Breach Notification Rules. The Plan is subject to HIPAA as are most health care plans, payers, and providers, such as hospitals, doctors, clinics and dentists. Most Apps will <u>not</u> be subject to HIPAA.

You can find more information about your rights under HIPAA and who is required to comply with HIPAA here: https://www.hhs.gov/hipaa/for-individuals/index.html.

Most Apps will fall under the control of the Federal Trade Commission (FTC) and the protections provided by the FTC Act. The FTC Act, among other things, protects against deceptive acts (e.g., if an App uses or discloses Personal Information in violation of its privacy policy).

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://reportfraud.ftc.gov/#/

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.

Last Revised: 7.21.23