Patient Quick Guide: Accessing Your Data with an App

- **What this means for you:** This feature allows you to use a third-party mobile app (an app not created by Highmark) to access and manage certain health information maintained by Highmark, including claims, clinical information, and prior authorization information.

- **CRITICAL PRIVACY NOTE: Once you share your health data with a third-party app, that data may not be subject to HIPAA. Its privacy policy – not HIPAA – will generally govern how your information is used, shared, or disclosed.**

- **Your Action:** We strongly urge you to read the detailed privacy warnings and checklist below to learn how to choose a safe and trustworthy application before connecting your data.

Covered Health Plan Patient Access API

Covered Health Plan is required to provide you with access to detailed information about your health history through a "Patient Access API" (Application Programming Interface) - a secure electronic connection for sharing data. While you are enrolled, and in some cases after you change coverage, you may access this information by downloading a third-party application (App) on your smartphone, 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 certain lines of business since January 1, 2016 (see footnote below). The information available, to the extent maintained in our records, may include:

- Claims and encounter data[2] concerning your interactions with health care providers;
- Clinical data that we collect in the process of providing case management, care coordination, or other services to you; and
- Prior authorization status, decisions, and related information, where applicable.

Certain information may be available for a defined historical period consistent with applicable regulatory requirements.

The information we will disclose may include information about treatment for substance use disorders, mental health treatment, HIV status, or other sensitive information.

It is important for you to understand that the App you select will have access to all of your information made available through the Patient Access API. The App generally may not be subject to the HIPAA Rules that protect health information held by covered entities and their business associates. Instead, the App's privacy policy describes self-

imposed limitations on how the App will use, disclose, and (possibly) sell information about you. 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.

Covered Health Plan does ask App developers to attest to basic privacy and security standards; however, this attestation is not legally required. If an App does not complete this attestation, we will inform you of that so you can make an informed decision about whether to continue using that App.

Please be advised that Covered Health Plan does not monitor or control how a particular App can use or disclose your data. 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 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 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?

- [1]Covered Health Plan means an entity issuing an insurance plan or product that is subject to CMS oversight and is within the scope of the CMS interoperability requirements, including Medicare Advantage organizations, state Medicaid and Children's Health Insurance Program (CHIP) fee-for-service programs, Medicaid and CHIP managed care plans, and Qualified Health Plan issuers on the Federally Facilitated Exchanges, as applicable.
- [2]Encounter data is information about office visits and other interactions with providers that are paid for under a fee that Covered Health Plan pays a provider for furnishing care to members.

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.

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. Covered Health Plan is 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 comply with 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. To file a complaint with Covered Health Plan about its compliance with HIPAA requirements, please call the customer service number located on the back of your member ID card. For App-related questions or concerns, contact the App developer directly; to file a complaint about an App's handling of your data, contact the FTC as shown below.

Apps and Privacy Enforcement

An App generally may 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 or security laws. The Federal Trade Commission protects consumers 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://ReportFraud.ftc.gov.

Important Note on Electronic Access

The Patient Access API supports electronic access to your health information and is part of broader efforts to improve interoperability. These capabilities are intended to improve efficiency and reduce reliance on manual processes such as phone, fax, and payer portals, but do not eliminate those processes.

Relationship to Other Interoperability Tools

The Patient Access API is part of a broader set of interoperability capabilities required by CMS. Additional tools are available to support:

- Provider access to patient information for care coordination (Provider Access API)
- Data sharing between health plans when coverage changes (Payer-to-Payer API)
- Electronic prior authorization processes (Prior Authorization API)

These capabilities are designed to improve access to information, enhance coordination of care, and reduce administrative burden across the health care system.