Patient Quick Guide: Connecting Your Health History

- **What this means for you:** You can request that Highmark securely transfer your health history from your previous or concurrent health plans so you can access health information from your current and prior health plans in one place.

- **Your Choice (Opt-In):** You are in complete control. This data transfer only happens if you give us your explicit permission (opt-in).

- **Your Action:** Sign in to My Highmark. Under Account Management, select Health data sharing to provide consent and information about the prior or concurrent health plan from which you want Highmark to request records.

Payer-to-Payer Data Exchange

The Payer-to-Payer Data Exchange Rule requires a Covered Health Plan to assist you with retrieving your clinical data from your chosen prior health plan and make the retrieved information available to you through interoperable technology.

Beginning in 2027, Covered Health Plans are required to support standardized electronic data exchange using a Payer-to-Payer API (Application Programming Interface) - a secure electronic connection for sharing data - which enables secure sharing of data between health plans when a member changes coverage. These capabilities are intended to improve continuity of care and reduce the need for duplicate information collection.

A Payer-to-Payer API request is always member-initiated and authorized by the member before any exchange of data between payers. The member must initiate their Payer-to-Payer request with their current payer and indicate their prior or concurrent payer for the data exchange to occur between the two payers.

With member authorization (opt-in), payers must exchange the following information, to the extent maintained:

- Claims and encounter data concerning your interactions with health care providers

- Clinical data (consistent with CMS-defined USCDI standards)

- Prior authorization history and related information, where applicable.

After the exchange occurs, members may access their data through tools such as the Patient Access API, including through a third-party application of their choice.

How to Initiate a Request

Before initiating a request, please have the following available:

1. Member portal login credentials with your current health plan
2. Member information that identifies your chosen prior or concurrent health plan
    a. If the information provided cannot be validated, the prior or concurrent health plan may require additional information for identity verification.

To initiate your Payer-to-Payer request, please sign in to My Highmark with your credentials. Navigate to the "Account Management" section. Provide your prior or concurrent health plan information, and provide your consent for Highmark to then initiate the data transfer.

Important Information

- Payer-to-Payer data exchange requires your authorization (opt-in) before any information is shared.
- Only information maintained by the prior payer and available under applicable standards will be exchanged.
- These electronic data exchange capabilities are intended to improve efficiency and reduce reliance on manual processes, but do not eliminate other methods of information sharing.
- Interoperability-enabled data exchange depends on factors such as payer connectivity, identity verification, and system readiness. Data may not be immediately available.

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.

Relationship to Other Interoperability Tools

The Payer-to-Payer 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)
- Member access to health information (Patient Access 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.