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 Patient Access API. While you are a current member, you may then access this retrieved information from your prior health plan by downloading a third-party Application (App) on your smart phone, tablet, computer, or other similar device. For more information on the Patient Access API, please visit **PATIENT ACCESS TO HEALTH INFORMATION**.

A Payer to Payer request is always member initiated and authorized by the member prior to any exchange of data between payers. The member must initiate their Payer to Payer request with their current payer and indicate who their prior payer was to their current payer for the data exchange to occur between the two payers. Only the member's clinical data in accordance with the CMS defined USCDI V1 standards is in scope for the P2P data exchange. API is the only permitted method for exchanging a member's data between two payers. Member's date of disenrollment from their prior payer must not be greater than 5 years from the current date for a member to be eligible to initiate a Payer to Payer request on that date.

Please visit (The URL is separate for each of HMK's entity. HMK PA URL: https://healthhist.com/highmarkbcbspa; HMK WV URL: https://healthhist.com/highmarkbcbswv; HMK DE URL: https://healthhist.com/highmarkbcbsde) to initiate your Payer to Payer request. After initiating your Payer to Payer data exchange request with your current payer, please allow at least 24 hours for your current payer to make your data retrieved from your prior payer available to you through the Patient access API.

Prior to initiating your request, please be sure to have available your-

1. Member portal login credentials with your current health plan
2. Member portal login credentials with your chosen prior health plan
    a. If your portals credentials with your prior health plan is invalid, they may require you to provide additional proof for validation.

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 ***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 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://www.ftccomplaintassistant.gov/#crnt&panel1-1.