Data Sharing

Interoperability and API Access

At the Community Mental Health Partnership of SE MI (CMHPSM), we are committed to providing our beneficiaries with secure, seamless access to their healthcare data in compliance with CMS interoperability requirements. As part of the ONC 2015 Edition Cures Update (170.315(g)(10)), CMHPSM ensures that beneficiaries and approved third-party developers can access health data through our secure APIs.

HIPAA Protections and Your Healthcare Data

At the CMHPSM, we are committed to safeguarding your healthcare data and ensuring it is handled in accordance with the Health Insurance Portability and Accountability Act (HIPAA). HIPAA provides critical protections for your personal health information (PHI), ensuring that it remains private, secure, and accessible only to authorized individuals or entities. Below is an overview of your rights under HIPAA and how to learn more about your protections.

Your Rights Under HIPAA

As a beneficiary, HIPAA grants you specific rights over your healthcare data, including:

- **Right to Access**: You have the right to access your healthcare information and request copies of your medical records from covered entities like health plans and healthcare providers.
- **Right to Request Amendments**: If you believe that your healthcare data is incorrect or incomplete, you have the right to request amendments to your health records.
- **Right to Privacy**: Your healthcare data is protected from unauthorized disclosure. Covered entities must follow strict privacy and security standards to ensure your information is only shared with authorized parties.
- **Right to File a Complaint**: If you believe your healthcare privacy rights have been violated, you have the right to file a complaint with the U.S. Department of Health & Human Services (HHS) Office for Civil Rights (OCR). You can learn more about how to file a complaint here.

For more detailed information about your HIPAA rights, visit the official CMS webpage: https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html.

Important Notice: Third-Party Applications and HIPAA

While your healthcare data is protected under HIPAA when it is in the hands of covered entities such as health plans or healthcare providers, **third-party applications** that you choose to use for accessing your healthcare data may not be required to follow HIPAA protections. This means that

once you authorize a third-party app to access your data, it may not be obligated to adhere to the same privacy and security rules that health plans and providers must follow.

Before choosing a third-party application, make sure to carefully review its privacy policy and understand how your data will be handled. If you have concerns about how an app may use or share your personal information, you may want to consider alternative options or limit the data you share.

For more information about the use of third-party apps and how HIPAA applies, please visit this HHS page: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access-right-health-apps-apis/index.html

Understanding Our APIs

The CMHPSM offers two distinct APIs to meet the CMS interoperability requirements and provide both beneficiaries and developers access to critical healthcare information. Below is a brief overview of each API:

Patient Access API

The **Patient Access API** is designed to allow CMHPSM beneficiaries to access their personal healthcare data securely. This API enables beneficiaries to retrieve a wide range of information from their health plan, including claims, encounter data, clinical information, and formulary data.

Key features of the Patient Access API:
- Provides secure access to health data such as diagnoses, treatments, and prescriptions.
- Allows third-party applications to retrieve patient data with the beneficiary's consent.
- Empowers beneficiaries to share their health information with trusted applications to manage their care.

The Patient Access API supports the CMS mandate for giving patients more control and transparency over their healthcare information. This API provides a standardized method for patients to securely view and manage their data, enhancing the overall healthcare experience.

Provider Directory API

The **Provider Directory API** is designed to help CMHPSM beneficiaries and developers access a comprehensive directory of in-network healthcare providers and pharmacies. This API allows beneficiaries and third-party applications to easily query information such as provider names, contact details, specialties, and locations.

Key features of the Provider Directory API:
- Allows beneficiaries to search for providers and pharmacies covered by their health plan.
- Supports third-party applications in displaying accurate provider details.
- Helps beneficiaries find the right healthcare professionals and services to meet their needs.

The Provider Directory API plays a crucial role in promoting transparency and ease of access to in-network providers, ensuring that beneficiaries can make informed choices about their care.

Educating Beneficiaries: How to Safely Select Third-Party Applications

Choosing the right third-party application to access your healthcare data is an important decision that can impact your privacy and security. At CMHPSM, we want to ensure that you make informed choices about which apps you use. Here are key considerations to keep in mind when selecting and using a third-party application:

- **Understand How the App Works**: Make sure you fully understand how the app operates and how it will allow you to access your personal health information (PHI). Review any guides, FAQs, or tutorials provided by the app developer to ensure you know how to navigate the app and manage your data.
- **Password Protection and Security**: The application should require strong password protection or multi-factor authentication for accessing your information. This adds an extra layer of security and ensures that only you (or someone you trust) can access your data.
- **Review the Privacy Policy**: A transparent, easy-to-read Privacy Policy is essential. It should clearly explain how your personal and health information will be used, stored, and shared. Be cautious of apps that either lack a Privacy Policy or have unclear terms. Ensure the policy outlines how changes will be communicated to you, and always look for apps that prioritize your consent.
- **Know What Data the App Collects**: Beyond your healthcare data, check what other types of information the app collects. Some apps may request access to your location, contacts, or even details about family members. If you're uncomfortable with the extent of data collection, consider looking for an alternative.
- **Where and How Data Is Stored**: Understand where your data will be stored and whether it is transferred or accessed outside the United States. Knowing the app's data storage practices is crucial in ensuring your data is safe and governed by appropriate legal protections.
- **Third-Party Sharing**: Review the app's policy on data sharing. Some apps may sell or share your information with advertisers, researchers, or other third parties. Ensure the Privacy Policy specifies who they share your data with and why. If you prefer not to share your data with third parties, look for an app that allows you to opt out of this practice.
- **Limit Data Use and Disclosure**: Make sure the app allows you to control how much data you share and with whom. Reputable apps will let you limit access to only the information necessary for the app's function, without forcing you to share everything.

- **Security Measures**: Verify that the app uses industry-standard security protocols like encryption to protect your data. Your health information should be safeguarded with reasonable and appropriate measures to prevent unauthorized access or breaches.
- **Handling Complaints and Issues**: The app should have a straightforward and transparent process for handling user complaints or privacy concerns. Make sure you can easily contact their support team if issues arise.
- **Ending Data Access**: If you decide to stop using the app or want to withdraw its access to your healthcare data, the app should offer a clear, simple process for terminating access. It's also important to check if the app has a policy for deleting your data once access is revoked, ensuring your information doesn't remain in their systems longer than necessary.

By following these guidelines, you can choose a third-party app that keeps your health information secure and gives you control over how your data is accessed and shared.

Beneficiary Access to Healthcare Data

CMHPSM offers access to healthcare data specifically for our beneficiaries. To access this data, beneficiaries will need to download and use a third-party application that connects to our healthcare data API. While no third-party applications are currently registered and available, we are actively accepting requests from app developers to integrate their software with our system, providing beneficiaries with easy and secure access to their health records.

Partnering with PCE Systems for Interoperability

In our ongoing effort to meet CMS interoperability standards, CMHPSM collaborates with our EHR vendor, PCE Systems. Together, we ensure the secure and compliant sharing of healthcare information in a way that meets the needs of our beneficiaries while protecting their privacy.

Security and Privacy Measures

Security is a top priority at NMRE, especially when it comes to healthcare data. We are fully compliant with HIPAA and CMS requirements to protect sensitive information. Our API features multiple layers of security, including:

- **Encryption**: All data exchanged via our API is encrypted to ensure confidentiality.
- **Authorization and Pre-registration**: Third-party developers must go through a pre-registration process to gain access to individual beneficiaries' data. Beneficiaries maintain full control over who can access their health information.
- **Token-based Authentication**: Access to data requires token-based authentication, adding an extra layer of security for every transaction.

API Information

Web Service API Documentation link: https://www.pcesystems.com/g10APIInfo.html

If you are a developer interested in connecting your application to our API, please review our Web Service API Documentation for full details on the security protocols and technical requirements. To apply for access to the API, please submit a written request using the PCE API Access Request Form in Appendix A of our Web Service API Documentation.

Provider Directory API
Endpoint: https://fhir.pcesecure.com:9443/PCEFhirServer/CMHPSM/metadata

Patient Access API endpoints are only available to application developers for security reasons. Please see the information above regarding how to access data via third party applications or how to apply for API access as a developer.

For any questions or support with the provided materials, please contact the CMHPSM Help Desk: help@cmhpsm.org