Accessing Member Health Information

Interoperability and Member Health Data:

You can now access your health data with any approved consumer health application (app).

As a member of Sacramento County Behavioral Health Plan (BHS), you can view your behavioral health information through a member chosen approved third-party app. By accessing your behavioral health information in this way, it provides new ways to engage with and manage your overall health.

Member Rights and Risks:

Right to share data with third-party apps

You can grant consent to share your behavioral health data with any chosen third-party app. When you consent, we are required to make your behavioral health data available to the third-party app within one (1) business day.

However, for the third-party app to access your data, the third-party app needs to register with Sacramento County.

There are no apps available currently, please check back in the future to view a list of registered apps and their risk scores.

Your rights under the Health Insurance Portability and Accountability Act (HIPAA)

A federal law called the Health Insurance Portability and Accountability Act (HIPAA) gives you the right to see and get a copy of your behavioral health record. Most health insurance plans and health care providers – including doctor's offices, clinics, hospitals, pharmacies, and labs – must follow this law. The U.S. Department of Health and Human Services (HHS) Office of Civil Rights (OCR) enforces the HIPAA Privacy, Security, and Breach Notification Rules, and the Patient Safety Act and Rule.

To file a complaint with the Office of Civil Rights, click here: Filing with OCR - HHS.gov

HIPAA and Data Sharing

The entities that must adhere to the HIPAA regulations "covered entities". These include:

- Health Plans, including health insurance companies, HMOs, company health plans, and Medi-Cal Managed Care Plans.
- Most Health Care Providers – those that conduct certain business electronically, such as electronically billing your health insurance (i.e., most doctors, clinics, hospitals, psychologists, and pharmacies.
- Health Care Clearinghouses – entities that process nonstandard health information they receive from another entity into a standard electronic format or data content.

There are also organizations that have health information about you who do not have to follow the Privacy and Security Rules. These include:

- Life insurers
- Employers
- Workers' compensation carriers
- Most schools and school districts
- Many state agencies like child protective service agencies
- Most law enforcement agencies
- Many municipal offices

Most third-party apps will **not** be covered by HIPAA. Most third-party apps will instead fall under the Federal Trade Commission (FTC) jurisdiction and the protections by the FTC Act. The FTC Act, among other things, protects against deceptive acts (e.g., if an app shares personal data without permission, despite having a privacy policy that says it will not do so).

The FTC has information about mobile app privacy and security for consumers, click on the link to learn more:

Does your health app protect your sensitive info? | Consumer Advice

To file a complaint with the Federal Trade Commission, click here: ReportFraud.ftc.gov

What are the risks?

Before you share your health information with a mobile app or third-party, look for the privacy policy that explains how it will use your health care data. Do not use the app if it does not have a privacy policy. If the app's policy does not answer the questions below, you should not share your health information with the app. Consider the following:

- What information will the app collect? Will this app also collect non-health information from my phone or computer, such as my location?
- How will my health information be saved?
- How will this app use my health information?
- Will this app share my information? If so, with whom and why?
- How can I limit the app's use of my health information?
- How does this app protect my information?
- Does this app have customer service contact information?
- How do I stop sharing my health information with the app?
- Will the app delete my information when I stop sharing it?
- Will the app let me know when there are changes to its privacy practices?

It is also important to know about the privacy settings on apps. When you download apps, they often ask for permission to access personal information like contacts, location, or even your camera. Ask yourself, does the app really need to access your location or photos to do its job?

Risk of secondary usage of data by the third-party apps

A specific example of risk to your data is called secondary usage. When your data is shared with and controlled by a third-party app, they may use your data in other ways, such as for advertising. Pay close attention to the privacy policy and user agreement provided by the app.

Risk of social engineering scams

Social engineering attacks, in which scammers try to access your health information, are becoming increasingly complex. Beware of people or organizations posing as representative of third-party health apps to trick you into sharing your sensitive information. Sometimes called "phishing scams," these could be phone calls or emails pretending to be a trustworthy company or person requesting your information.

You can protect yourself with these tips:

- Keep your anti-virus/anti-malware software updated.
- Use and check your email filters and spam filters.
- Use multi-factor authentication for important accounts.
- Don't respond to requests for personal information or passwords.
- Don't open email from a suspicious source.
- Don't click on links received in an email from a suspicious sender.
- Don't download or open attachments in an email from an unknown sender.
- Don't use the same password for multiple accounts.

For more information on how to protect yourself from social engineering scams, or if you think you may have been a victim of such a scam, visit Phishing Scams | Federal Trade Commission

Third party apps

Who manages third-party apps?

Third-party apps are managed by individuals or organizations outside of Sacramento County BHS.

Provider Directory

The Provider Directory Application Program Interface (API) is a recent development aimed at delivering current details regarding healthcare providers and facilities to members of the Centers for Medicare & Medicaid Services (CMS). Through this API, members can explore healthcare providers and facilities based on various factors such as location, specialty, and other criteria.

This API emerged as a response to the CMS Interoperability and Patient Access Final Rule. This regulation mandates health plans to furnish members with access to precise and promptly updated provider directory information through an API. The rule's objective is to enhance access to care and guarantee that members possess the necessary information to make well-informed decisions concerning their healthcare.

API Description

The Provider Directory guide is built on the Fast Healthcare Interoperability Resources (FHIR) and serves as the cornerstone of a comprehensive provider directory. It delineates the scenarios and search criteria for locating a practitioner or organization, while also specifying the essential data elements and offering fundamental query instructions. The elements outlined in this guide aim to establish groundwork for a centralized Provider Directory.

For more information about how to use the API, please refer to the API's Documentation:

CalMHSA Connex - California Mental Health Services Authority

Patient Access

As part of CMS Interoperability and Patient Access Rule, BHS implemented a publicly available Patient Access Application Program Interface (API) which seeks to establish members as the owners of their health information with the right to direct its transmission to third-parity applications.

API Description

The Patient Access API allows members to access their personal health information through a third-party application of their choosing. This API implements the HL7 Fast Healthcare Interoperability Resources (FHIR) implementation guides listed below.

https://hl7.org/fhir/us/carin-bb/

https://hl7.org/fhir/us/davinci-pdex/

https://build.fhir.org/ig/HL7/davinci-pdex-formulary/

For more information about how to use the API, please refer to the API's Documentation:

https://www.calmhsa.org/interoperability-api/