

Frequently Asked Questions: MO HealthNet IOX

- **What is the Interoperability and Patient Access Rule?**

The Centers for Medicare & Medicaid Services (CMS) requires MO HealthNet to offer a **Patient Access Application Programming Interface (API)**, to allow MO HealthNet participants easy access to your claims and health information through a third-party application (app) of your choice. The Missouri Department of Social Services implementation of this rule is called “MO HealthNet IOX.” The rule also requires MO HealthNet to offer privacy and security resources to you.

- **What is a third-party application?**

A third-party application is an interface that is developed, managed, and maintained by an outside organization, **not** by MO HealthNet.

- **Will my health information be protected?**

The Health Insurance Portability and Accountability Act (HIPAA) requires your healthcare provider and MO HealthNet (Missouri Medicaid) to protect your health information. Because most third-party apps are not HIPAA-covered entities, they might not be liable for protecting your information or bound by the same rules and regulations as HIPAA-covered entities.

You **are not** required to use MO HealthNet IOX, but if you choose to you will be required to consent to giving personal and protected health information to a third-party app. It is important that you take the time to read and understand an app’s privacy policy and terms of service before giving them access to your personal data and health information.

- **What is personal information?**

Personal information is any information directly linked to you, including your:

- Name or date of birth
- Contact information (ex. address, phone number, email address, etc.)
- Social Security Number or Medicaid ID Number
- Provider ID Number
- Any combination of information that may be used to identify you

- **What is protected health information (PHI)?**

This is information about your health and healthcare. It may include:

- Past, present, or future physical or mental health conditions
- Written data from doctor’s visits about treatments, illnesses, disorders, etc.
- Provision of healthcare to an organization
- Future payment of the provision of healthcare to an individual

- **What are my responsibilities when it comes to my information?**

Once you choose an app, it is your responsibility to read and understand the app's privacy policy, terms of service, and other relevant information so you are aware how the app is permitted to use or even sell your private and protected information to other organizations and entities.

- **What third-party apps can be used to view my protected health information?**

Large, well-known companies, like Google or Apple, and small companies, like your hospital or physician's office, can use these apps. They are usually accessed from a phone or tablet.

- **What should I consider when choosing an app?**

Because certain health data can be shared by multiple people, you should consider how sharing your data with an app could affect others, such as family members. Please remember your health information is very sensitive.

MO HealthNet recommends reviewing the third-party apps' Privacy Policy and Terms of Service before installing it on your device. If the app does not have a privacy policy, you should consider a different app. Violations of these terms could be reportable to the Federal Trade Commission (FTC). The Privacy Policy should clearly answer questions like:

- Who is offering the app? How is it funded?
- What data will be collected? Will non-health data be collected, like my location?
- How will my data be used?
- Where will my data be stored? Will it be stored anonymously?
- Will I be notified about the data collected about me?
- Can I delete the data stored about me?
- Will third-party persistent cookies, also known as tracking cookies, be used? Tracking cookies are small text files that can track you, as you use the internet.
- Can the app sell or disclose my data to other organizations or entities? Am I able to limit this?
- Who can view my data when I consent to access?
- How can I correct inaccuracies, if I notice any?
- Is there a way for me to voice concerns or complaints?
- Will I be informed if there are changes that affect my privacy? If so, how?
- What security measures are used to protect my data?
- Can I terminate the app's access to my data once it has been granted?
- Will they still have access to my data if I terminate access?

- **What personal information do I have to provide?**

If you choose to use the MO HealthNet IOX solution, you will have to provide personal information necessary for registration, identification, and authentication purposes. This includes your:

- First and last name
- Address
- Phone number
- Valid email address
- Social Security Number
- Medicaid ID
- Date of birth

- **What are permissions?**

Apps need your permission to access to your location, contacts, camera, or microphone. Pay close attention to the permissions requested when you install an app or use it for the first time. These requests often come in the form of pop-up windows you must agree to.

Regularly updating an app can protect you from malware or out-of-date software that could be at a higher risk for hacking. Here are some tips to keep in mind:

- Only download apps from official app stores (like the Apple Store or Google Play) and research the developer before installing it
- Understand what information the app will request access to
- Check the permissions settings for requests like gaining access to your location, camera, or microphone (you can also review the app's permissions by selecting it in your device settings)

- **Can my personal representative access my data through the app I select?**

Designated personal representatives may access another individual's personal health information using an app if they have all of the correct information needed to register for or access the patient's MO HealthNet IOX portal.

- **Can I withdraw consent once I've given it?**

You can withdraw consent for a third-party app at any time. Please review the **MO HealthNet Member IOX User Manual** for instructions on how to withdraw your consent. Once you withdraw your consent, MO HealthNet will stop sending information to the app.

NOTE: We also recommend you also reach out to the app directly to ask them to delete your data.

- **What if the app returns inaccurate data?**

If an app returns healthcare data that appears inaccurate, please ask your MO HealthNet provider to call **573-751-2896** to report this issue with our team for review and follow up. Please note that our team can only help MO HealthNet providers.

- **Is there any accountability for third-party applications?**

Although most third-party apps are not HIPAA-covered entities, they are still required to comply with Federal Trade Commission (FTC) protections. If you believe there has been a breach with your data or it has been used inappropriately, you can report it to:

- The FTC at ReportFraud@ftc.gov
- MO HealthNet at MHD.Privacy@dss.mo.gov

- **Where can I find more information and resources?**

For more information about HIPAA rights and coverage, please visit:

- [Your Rights Under HIPAA | HHS.gov](#)
- [HIPAA FAQs for Individuals | HHS.gov](#)
- [Privacy forms | Missouri Department of Social Services \(mo.gov\)](#)

For more information about FTC protections, please visit:

- [Identity Theft & Online Security](#)

- [How To Protect Your Phone and the Data on It](#)
- [How To Protect Your Privacy on Apps](#)