How you can use your health data

Health plans are now required to provide you a secure way to access and share your health information.

On March 9, 2020, the Centers for Medicare & Medicaid Services released the Interoperability and Patient Access final rule. Final rule requires health plans to implement a secure application programming interface (commonly known as an “API”) that gives members easy access to their health information.

How it works

First, you must create a Personal Data Release account with your Health Plan.
With this new functionality, you can access your electronic personal health information via a third-party application (“app”) that has registered with your Health Plan. With your permission, the app will retrieve your personal health data from your Health Plan and make it available for you to view.

- **Why this matters**

  It is important to us that your health information is staying private and secure. You will use the username and password that you create for your Personal Data Release account to give your Health Plan permission to share your personal data with a third-party app. This helps ensure that your information will not be read or understood by someone who is not authorized to view it. This also helps your Health Plan keep a record of who has looked at your information, what changes were made and when. You will only need to set up your Personal Data Release account once.

Next, you need to find an app that you’d like to use with your device.
Read an app’s privacy policy carefully before you give it permission to use your health information. Follow recommendations to keep your information safe and protect yourself from scams, fraud and abuse. For the app to pull your data from your Health Plan, they will need to be registered with your health plan and connected to your health plan’s API. Since this is new technology, initially the number of third-party apps that have chosen to connect with your Health Plan may be limited.

- **Keep in mind**

  Depending on your device operating system, you can browse apps in Apple’s App Store or Google Play Store. Apps may also charge you a subscription fee.

It is your responsibility to protect your personal health information once you download it from your Health Plan.
Your Health Plan, takes your privacy and security seriously. Once you download your health information the Health Plan, it's important for you to keep it as safe and secure as possible.

Choosing an app

Your health information is very sensitive information. Be careful to choose apps with strong privacy and security standards to protect it. Ask yourself the following questions when you consider giving an app permission to use your information.

- What health data will this app collect? Will this app collect non-health data from my device such as my location?
- Will my data be stored in de-identified or anonymized form?
- How will this app use my data?
- Will this app disclose my data to third parties?
    - Will this app sell my data for any reason, such as advertising or research?
    - Will this app share my data for any reason? If so, with who? For what purpose?
- How can I limit this app's use and disclosure of my data?
- What impact could sharing my data with this app have on others, such as my family members?
- What security measures does this app use to protect my data?
- How can I access my data?
- Does this app have a process for collecting and responding to user complaints?
- What is the app's policy for deleting my data once I terminate access? Do I have to do more than just delete the app from my device?

If an app's privacy policy does not clearly answer these questions, then you should reconsider using that app to access your health information.

Keep your information safe

In order to keep your personal health information safe, you must take an active role in protecting it. Follow these safety precautions when viewing and managing your information.

- Never access your health or financial information on a public Wi-Fi network, such as at a public library or coffee shop.
- Use a unique username and password for each of your devices and accounts.
- Update your passwords regularly. Do not use the same password for multiple accounts.
- Choose PINs that do not show up in your wallet. For example, do not use your birthdate or address.

- Keep up with software updates. These updates include regular security patches to help safeguard your information.

Protect yourself from scams, fraud and abuse

Staying informed and keeping your information secure is key to protecting yourself and others from scams, fraud and abuse. Here are tips to avoid potential fraud and abuse.

1. Keep your ID cards and personal information secure at all times.
2. Be alert for recent health care scams. Television, newspapers, social media and trusted sources online can provide you with credible information on recent schemes.
3. Review your health care documents to ensure they are accurate.

If you suspect that you may have been involved in a fraud or abuse incident, or if you receive information that isn't what you expected or doesn't make sense to you, report it right away.

- Contact your Health Plan's Compliance team.
- File a HIPAA complaint at Filing a HIPAA Complaint.

What is HIPAA?

The Health Insurance Portability and Accountability Act, also known as HIPAA, is the federal law that sets rules for health care providers and health insurance companies, like your Health Plan, on who can look at and receive your health information. Your health information can be used and shared for specific reasons, not directly related to your care, like making sure doctors give good care, making sure nursing homes are clean and safe, reporting when the flu is in your area, or reporting as required by state and federal law.

HIPAA regulations protect and secure your health information when it is held by your health care provider (such as your doctor or hospital) or your Health Plan. HIPAA **does not apply** to your health information once you authorize a third party to access it.