

3 Common MYTHS ABOUT MOBILE HEALTH APPS

YOUR HEALTH DATA MIGHT BE AT RISK!

CURRENT EFFORTS

These resources can help you find apps that have shown minimum standards are met, including some that follow HIPAA rules.

Medicare App Library*

Medicare Connected Apps Directory (Blue Button) *

Third-party apps that connect to Medicare

All the digital applications (apps) in this collection have been developed by private companies and:

- **Prioritize your privacy:** Independently verified to ensure they meet high standards for protecting and exchanging your health information.
- **Keep your information secure:** Identity verification is built in, and they'll never sell or share your data.
- **Require your permission:** Can only access the Medicare data you choose to share.



CMS Blue Button API

Blue Button is a standards-based application programming interface (API) that delivers Medicare Part A, B, and D data for over 60 million people with Medicare.

Get started →

API reference {}

For People with Medicare

Learn about Medicare's Blue Button & find apps you can use.

Get details on Medicare.gov

*Specifically for those covered by Medicare, but may be referenced by all



THINK BEFORE YOU CLICK!

FIVE TIPS TO HELP YOU PROTECT YOUR HEALTH DATA AND STAY SAFE WHEN USING HEALTH APPS*

- 1. DOWNLOAD FROM TRUSTED APP STORES AND USE A STRONG PASSWORD**
Official app stores are more likely to have healthcare apps that have gone through the minimum security review of first-party stores. Use a unique and strong password when you create an account with a health app.
- 2. CAREFULLY READ THE PRIVACY TERMS AND CONDITIONS**
While the legal writing may be confusing, understanding if the app is protected by federal law or is storing your sensitive health data in a vulnerable place can help protect you from someone stealing your data.
- 3. FIND OUT WHAT DATA THE APP IS COLLECTING**
Not every app collects just the data you think it's collecting. Make sure you understand exactly what data they capture and store before you click accept on data sharing prompts.
- 4. DETERMINE WHERE THE APP WAS DEVELOPED AND DATA IS STORED**
Who develops and where the app was developed could impact how they use, store, and share your sensitive health data. If you are uncomfortable with who the developer is or where the app was developed choose an alternative.
- 5. KNOW IF THE APP SHARES OR SELLS YOUR DATA**
Some applications – especially ones marketed as free – make money by sharing or selling your data, sometimes without you even knowing it. Be sure you know what the app is doing with your data and never authorize the app to share your data on social media.

*For more information on U.S. government resources or to report data misuse visit www.consumer.ftc.gov

Think Before You Click

Follow these additional free tips to protect your data.



FIND IT AT WEDI.ORG

MYTH: MY SLEEP TRACKER PROTECTS MY DATA THE SAME WAY MY DOCTOR DOES

FACT: Apps (like your patient portal) offered by a doctor, hospital, other provider, and health insurers are required to follow HIPAA privacy & security rules.

Standalone mobile health apps might not follow the same rules.

MYTH: AI HAS TO KEEP MY DATA PRIVATE

FACT: Some artificial intelligence (AI) products may use your data to train their models or otherwise share it.

If you are uncomfortable with your private data potentially being used in this way, consider how you want to use AI tools.

MYTH: ALL MY HEALTH APPS ARE SAFE TO USE AND WILL PROTECT MY DATA

FACT: While some voluntary efforts are underway, there is not yet a universal privacy & security approval process for mobile health apps. Only those covered by the HIPAA law have to protect your data in the same way a doctor, hospital, other provider, or health insurer does.