Make sure your personal information is safe on third-party apps

Questions and answers about privacy

Your privacy matters to us. CareOregon wants to make sure your health data is safe. Please read this important information about keeping your protected health information (PHI) secure.

Q: Is my data safe with CareOregon?
A: Yes. The systems we use to store and access your PHI are secure, private and updated often. We follow the rules of the Health Insurance Portability and Accountability Act Privacy Rule (HIPAA). HIPAA requires us to adopt specific measures to protect your health data. Our systems are HIPAA-compliant, and our staff is trained to keep your PHI safe. Your health data is safe with us.

Q: How does HIPAA protect my health data and privacy?
A: HIPAA requires health care companies like CareOregon to follow best practices to safely store your data in our computer systems. It also limits how this data can be used or shared. For example, HIPAA does not allow CareOregon — or any health care company — to sell your data or use it for ads. HIPAA also requires we notify you quickly if your health data is breached, and it imposes penalties on health care companies that don't protect your data.

Q: What kind of third-party apps can access my PHI?
A: There are many apps for your smart phone, tablet or mobile device that can help you manage your health, including:

- Calorie counters.
- Workout and fitness trackers.
- Sleep monitors.
- And more.

Some of these apps may offer features like setting up reminders for medications, tests and appointments, or being a place where all your health information can be stored in one place. Such apps might ask you to access your health information stored with CareOregon or your providers so you can view and manage this information through the app. You have a right to ask your plan or provider to share your information with the app of your choosing. While these apps can be useful tools, they may put your PHI at risk.

Q: Is my information safe with third-party health apps?
A: Once you allow an app to receive your health information from us, we are no longer able to protect that information for you. This includes apps you currently use or are thinking of using. Whether your information is safe with a third-party app depends on the policies and practices of the app you choose. It is important to read an app's privacy policy to make sure the app handles your data safely and does not sell or share your information without your permission. More ways you can keep your information safe before and after you install an app can be found here.

Q: If I give a third-party app access to my health information, do they have to follow HIPAA?
A: No. Most third-party apps do not have to follow HIPAA's safeguards. The data you share with a third-party app may not be protected by HIPAA. When stored in a third-party app, your health data falls under the oversight of the Office of Civil Rights and the Federal Trade Commission (FTC). In particular, the FTC protects against deceptive or unfair practices, including:

- Those relating to privacy and data security.
- Those involving false claims about apps' safety .

For example, the FTC protects against fraud, like an app sharing your personal data even though their privacy policy says they won't. For more information about the FTC and third-party apps, visit consumer.ftc.gov/articles/how-protect-your-privacy-apps

Q: What are some other steps I can take to protect the privacy and security of my health information when using a third-party app?
A: Make sure to follow basic best practices for keeping data safe, like using strong passwords and not sharing login information with other people. You can also make sure your smart phone has a lock code or uses face ID or fingerprints to unlock.

Q: Should I share my health data with third-party apps?
A: It is up to you, but we want you to have as much information as possible before you decide. Below are some questions to think about before you give a third-party app access to your health data. If you're not satisfied with the app's answers to these questions, we recommend not giving the app access to your health data.

- Does the app have a clear, simple privacy policy? How do I know when the policy changes?
- How will the app use my data? Is it worth the risk?
- What health data will the app collect? Will the app collect other information, like my location?
- Is my data made secure through encryption or making it anonymous?
- Where will my data be stored? Will it be within the U.S. or in a foreign country?
- Who owns the app and where are their headquarters? Are they subject to U.S. laws?

- Will the app share or sell my data to other apps or companies?
- Will my data be used for targeted ads?
- Will sharing my data on the app affect anyone else, like my family?
- Does the app let me change my mind about sharing my data or easily make complaints?
- If I stop using the app, can I end or block their access to my data?
- If I stop using the app, will they permanently delete my data?
- If I stop using the app, will they allow me to export my data?
- If I die, can my family or heirs request that my data be permanently deleted?

Q: How can I make a complaint about third-party apps?
A: There are a few different ways:

- Make a complaint about an app with the FTC: reportfraud.ftc.gov
- Make a complaint through the Office for Civil Rights: ocrportal.hhs.gov/ocr/smartscreen/main.jsf

Q: What if I have additional questions?
A: Feel free to contact CareOregon Customer Service at 503-416-4100, toll-free at 800-224-4840, TTY 711, or send us a secure message at careoregon.org/portal