Protecting the Privacy of Your Health Information: Interoperability and Third-Party Apps

Scott and White Health Plan (SWHP) and FirstCare Health Plans (FCHP) appreciate that your medical and health information is personal. We are committed to helping you understand how to protect the privacy and security of your health information when you're choosing how to access – and if to share – your health data.

The Centers for Medicare and Medicaid Services (CMS) guidelines for "interoperability" describe the authorized sharing of health information between health plans, their members and third-party applications (apps). According to CMS, the goal of interoperability is to give you access to your health information when you need it most, and in a way you can best use it.

The CMS guidelines for interoperability apply to programs such as Medicare Advantage plans, Medicaid and CHIP managed care, and Qualified Health Plans on the Federally facilitated Exchange. The guidelines require health plans like ours to enable members to access their health information through independent third-party apps, with member authorization.

As a health plan that participates in the interoperability initiative, we want to provide you with the following information about protecting your privacy and using third-party apps.

FAQs for Third-Party Apps

What should I consider before sharing my health information with a third-party app?

When choosing an app, be sure to look for an easy-to-read privacy policy that clearly explains how the app will use your health data. If an app does not have a privacy policy, you should not use that app. You should also consider these questions:

- What health data will this app collect? Will this app collect non-health data from my device, such as my location?
- 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?

- What security measures does this app use to protect my data?
- If I no longer want to use this app, or if I no longer want this app to have access to my health information, how do I terminate the app's access to my data?

If the app's privacy policy does not clearly answer these questions – and any other questions you may have – you should reconsider using this app.

What are my rights under the Health Insurance Portability and Accountability Act (HIPAA) and who must follow HIPAA?

HIPAA is a federal law that protects an individual's health information from being disclosed without the individual's consent or knowledge. The U.S Department of Health and Human Service (HHS) Office for Civil Rights (OCR) enforces the HIPAA Privacy, Security, and Breach Notification Rules. Learn more about HIPAA on the HHS website:

- Your Rights Under HIPAA
- HIPAA FAQs

Most third-party apps are not covered by HIPAA, but they fall under the purview of the Federal Trade Commission (FTC) and the FTC Act. The FTC Act protects against deceptive practices such as sharing personal data without permission, or sharing information in ways not in keeping with a privacy policy. Learn more about protecting your privacy on the FTC website:

- How to Protect Your Privacy on Apps
- Before You Install an App

What should I do if I think my health information has been used inappropriately?

If you have any concerns about how SWHP or FCHP may have violated your privacy rights, you can report your concerns and get help:

- Contact our member support team at the phone number printed on your ID card. Your issue will be reviewed by our Compliance team, who will follow up with you to discuss further.

You can also file a complaint about a HIPAA issue or a third-party app:

- File a complaint about a HIPAA issue on the HHS website: Filing a Complaint
- File a complaint about a third-party app on the FTC website: FTC Complaint Assistant