COMMON GROUND
HEALTHCARE COOPERATIVE

Using a Third-Party Application to Access Your Protected Health Information

To access your Protected Health Information ("PHI") using a third-party application (3rd Party App) that connects to Common Ground Healthcare Cooperative (CGHC), please read this important information.

We require 3rd Party Apps to provide us with written confirmation that they meet certain requirements when accessing CGHC member PHI. This process is called attestation and gives us confirmation that the 3rd Party App provider agrees to specific requirements to keep PHI confidential and secure.

As part of our commitment to your safety and proper use of your data, we have asked all application providers to review the following criteria and "attest" or declare that they meet or follow these criteria.

Security of Application

We ask providers of 3rd Party Apps to declare that their application does not have common security issues as defined by the Open Web Application Security Project (OWASP). If an application has any of the issues defined by OWASP, your health data could be placed at risk by hackers. Learn more here.

Privacy of Your Data

We also ask providers of 3rd Party Apps to declare that they have a privacy policy that is in line with common privacy practices within the healthcare industry. We do this by asking application providers to declare that they conform with the CARIN Code of Conduct. This Code of Conduct defines proper privacy policies that protect your data from improper use or sharing with 3rd parties. Learn more here.

Third-Party Applications must be approved by CGHC before they can be used to access member PHI. We do this to protect your PHI and the security of our systems.

Things to Consider when Choosing a *3rd Party App*

Understanding how a 3rd Party App uses, discloses, and stores your PHI and other health information is important. Ensuring the 3rdParty App keeps your personal information private and secure is critical. You should understand how the 3rd Party App protects the privacy and security of your health information before giving them access to your sensitive health information.

Below are some tips for choosing a 3rd Party App to access your PHI:

- How easy is the 3rd Party App to use for accessing your personal information?
    - Is a password required for you to access your personal information, and is two-factor authentication available?
    - Does the 3rd Party App have an easy-to-read Privacy Policy that clearly explains how they will use and disclose your personal information? The Privacy Policy should explain how you will be informed of any changes to the policy. If the 3rd Party App doesn't have a Privacy Policy, we recommend that you choose a different 3rd Party App.
- What PHI and other personal information will the 3rd Party App collect?
    - Will the 3rd Party App collect non-health information?
    - Will the 3rd Party App collect other information from your mobile device, such as your location or information about your family and/or friends?
    - Will your data be de-identified or anonymized?
- How does the 3rd Party App store and use your personal information?
    - Where does the 3rd Party App store your personal information? For example, will your personal information be stored in the United States, or will it be transferred or accessed outside the United States?
    - Does the 3rd Party App sell or share your personal information with third parties? If it does, the 3rd Party App's Privacy Policy should explain why and to whom.
    - Can you limit how the 3rd Party App uses and discloses your personal information?
    - What impact could sharing your data with this app have on others, such as your family members?
- Does the 3rd Party App have reasonable and appropriate security measures to protect your personal information?
- How can you access data and correct any inaccuracies that might exist?
- Does the 3rd Party App have a clear and easy-to-understand process to handle user complaints?
- If you no longer want to use the 3rd Party App, or if you no longer want the 3rd Party App to have access to your PHI, is there a clear and easy process to terminate the 3rd Party App's access to your PHI and other personal information?
    - Does the 3rd Party App have a policy for deleting your PHI and other personal information once you terminate the 3rd Party App's access?

Your Privacy Rights

As a healthcare consumer, you have privacy rights that are protected under law. The federal law that gives you these protections is called the Health Insurance Portability and Accountability Act (HIPAA). The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) enforces HIPAA.

HIPAA generally applies to covered entities that include health plans and health care providers, and "business associates" that provide service to those plans and providers. You can find more information about HIPAA at:

- HHS Guidance for Consumers
- HHS FAQs

To learn more about filing a complaint with OCR under HIPAA click here. To file a complaint please visit HHS Complaints.

IMPORTANT – HIPAA does not cover many 3rd Party Apps, particularly those that are offered directly to you, rather than those offered through a health plan or provider. This means your health information will not be subject to the same privacy and security protections that health plans and providers must adhere to.

Third-party applications are regulated by the Federal Trade Commission (FTC) and the protections provided by the FTC Act. However, if the 3rd Party App is located outside the United States, the FTC may not be able to fully protect your information. You can find more information from the FTC about 3rd Party App privacy and security at FTC Mobile Apps. If you think a 3rd Party App has misused or violated your privacy, you can file a complaint with the FTC using the FTC complaint assistance at ReportFraud.ftc.gov

INTEROPERABILITY "DATA SHARING" EDUCATION CONTENT

What is Interoperability?

Interoperability refers to a simple, standard method for members to access and share their health information (Electronic Health Records (EHR)/Personal Health Record (PHR) and/or encounters) with the utmost security. In other words, interoperability is "Data Sharing" between the healthcare patient, the health insurance company, and software applications on smart devices or computers.

Why Interoperability?

The goal of Interoperability is for patients to receive better quality of healthcare and outcomes by sharing their personal health information with their provider(s) and using that information for personal health tracking.

Health insurance companies, like Common Ground Healthcare Cooperative (CGHC), store member information on computer servers. As patients move from one healthcare provider to another, their health information must be available with ease of access. Third-party applications provide an easy way for patients to access, exchange, and integrate their health information between different healthcare provider systems.

Important: if you have been insured by other health insurance companies, between January 1, 2016, and today, you will need to contact each insurer to access and share the health data they hold for you.

How to Access Your Health Information?

1. Register with the Common Ground Healthcare Cooperative on the HealthLX web portal
2. Login to the application using the credentials established during registration
3. Choose your preferred third-party application from the list.
4. Provide your consent for the application to access your health information.

As a CGHC health insurance member, you have access to:

- Claims submitted by your provider(s)
- Pharmacy data

Is the data current in the HealthLX web portal?

CGHC will provide access to your healthcare data within 48 hours of receiving the information from providers. Keep in mind that the time between when you receive a healthcare service and when CGHC receives the claim can vary.

How much of my data history can I access?

Data from January 1, 2016, onward must be available to the member. This follows the U.S. Centers for Medicare & Medicaid Services (CMS) guidelines.

How do I stop the third-party application from accessing my health information?

- Option 1: Log into each third-party application that you want to stop sharing your CGHC health information with. Follow their instructions for disconnecting from the HealthLX web portal.
- Option 2: Contact CGHC Member Services and ask that your HealthLX account be locked. This will prevent all linked third-party applications from accessing your CGHC health information. Important: This will also prevent you from logging into your HealthLX account.