USING A THIRD-PARTY APPLICATION TO ACCESS YOUR PROTECTED HEALTH INFORMATION

If you want to use a third-party application (3rd Party App) that connects to Common Ground Healthcare Cooperative (CGHC) to access your protected health information ("PHI"), please read this important information.

Common Ground Healthcare Cooperative (CGHC) requires 3rd Party Apps to provide us written confirmation that they meet certain requirements when accessing CGHC member PHI. This process, called attestation, gives us confirmation that the 3rd Party App provider agrees to specific requirements to keep PHI confidential and secure. You can view this attestation by clicking here: "Interoperability: Third-Party Application Registration Statement".

3rd Party Apps must be approved by CGHC before they can be used to access member PHI. If there is an app you would like to use but has not been approved yet, you can request a review of the app by clicking here and following the instructions to complete the request.

If the *3rd Party App* you want to use does not agree to our attestation or does not respond, we will not allow it to access your data. You can change your mind about using the *3rd Party App* to get your PHI from us. If you do not respond timely, letting us know if you've changed your mind, then we will share your PHI with the *3rd Party App*, in accordance with applicable law. If the *3rd Party App* is a risk to the security of CGHC's information systems, we will not allow the *3rd Party App* to connect to our systems and your PHI will not be shared with the *3 rd Party App*. In order to protect your PHI, we recommend only using a *3rd Party App* that has agreed to CGHC's attestation.

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

It is important that you understand how a *3rd Party App* uses and discloses your personal information, which may include PHI and other health information. It is also important that the *3rdParty App* you choose keeps your personal information private and secure. Below are some tips on information to look for and ask when choosing a *3rd Party App.*

- Do you understand how to use the *3rd Party App* to access your personal information?
- Does the *3rd Party App* require the use of passwords for you to access your personal information?
- Does the *3rd Party App* have an easy-to-read Privacy Policy that clearly explains how the *3rd Party App* 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* does not 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?
- 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?
- Does the *3rd Party App* have reasonable and appropriate security measures to protect your personal information?
- 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 your 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 health information is very sensitive information, and you should understand how *3rd Party Apps* protect the privacy and security of your health information.

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, please visit HHS Complaints.

It is important to understand that many *3rd Party Apps* are not covered by HIPAA, particularly those that are offered directly to you as an individual, rather than 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. *3rd Party Apps* 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 able to fully protect your information. You can find more information from the FTC about mobile *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 FTC Complaint Assistance.

Interoperability "Data Sharing" Education

Interoperability: An easy way to access and share your health information with utmost security.

Interoperability means "Data Sharing" between the healthcare patient, the health insurance company, and software apps on smart cellphones or computers. Healthcare insurers must provide members an easy, standard, and secure method to access their health information from third-party apps.

Health insurers store the member information on computers. As patients move around from healthcare provider to provider, or for other healthcare uses, their health information must be available with ease of access.

Significance of Interoperability:

- US federal Government required patient's rights
- Members can easy access to their health information with security standards.
- Caregiver can access to their patient's information, and parents can access their dependents health information
- Data Integrity across health systems.
- Allows for improved quality healthcare services

It depicts data sharing between Member, insurer, Member App, providers (Doctor, Hospital, Personal trainer, Nutritionist, and LAB)

Frequently Asked Questions

What is Interoperability? Interoperability is an easy way to exchange, access and integrate Health information (Electronic Health Records (EHR)/Personal Health Record (PHR) and/or encounters) across systems securely. The access can be within any health system, and your app can access the insurers' system to receive your health Information.

Why Interoperability?

Common Ground Healthcare Cooperative (CGHC) is compliant with the federal government regulatory guidelines, which has a roadmap to take the healthcare Industry to next level of health care management by easy and secure access to healthcare information. With easy access to your health information, you can receive quality healthcare service and outcomes by sharing information with the provider and using it for tracking personal health.

How to access Health Information?

As a CGHC member, just follow below 3 steps to access your health information:

- Register with CGHC's Connected Health web portal
- Choose your preferred application available in the list
- Login to the application using the credentials established during registration and provide consent to access your health information.

What are all the health information member can access?

As a valued CGHC member, you have access to below health information:

- Claims submitted by your provider
- Pharmacy subscription data

How current will the data in the Connected Health portal be?

As per the CMS guideline, members can access their data 24 hours a day. CGHC will provide access to data within 48 hours of receiving information from providers. The time between office visit and info sent to CGHC varies by provider.

How much History of data Member can access?

Following the CMS guideline, CGHC members can access the data from January 1, 2016.

I am using an application to receive Connected Health information; how do I stop the application from accessing my health information?

Login to the Connected Health portal, click Profile and Settings and then click Linked Services. Then click the Manage Your Apps button to see which apps you have connected with and to revoke access as necessary. Once the application's consent has been revoked, you will not be able to access your information through the application.