Group Health Cooperative of South Central Wisconsin
Attn: Privacy Officer
1265 John Q. Hammons Drive
Madison, WI 53717

Date

Parent/Guardian of
NAME
ADDRESS
ADDRESS 2
CITY STATE ZIP

Notice of Data Breach

Group Health Cooperative of South Central Wisconsin (GHC-SCW) takes the privacy and security of the information in our possession seriously. Unfortunately, we are writing to inform you of a recent security incident that involved some of your personal information. We want to reassure you that we have fully investigated the situation and taken all necessary steps, the last of which is sharing the details with you in this letter.

You may be aware that on January 25th, 2024, we posted an announcement on our website informing you that we had identified unauthorized access to our network by an unknown attacker. Below we will share the specific information about this incident, a description of what we have done to investigate and correct it, and information about how we can assist you.

What happened?

In the early morning hours of January 25th, 2024, GHC-SCW identified unauthorized access to our network. Our Information Technology (IT) Department purposefully isolated and secured our network, causing several of our systems to be temporarily unavailable. The attacker attempted to encrypt GHC-SCW's system but was unsuccessful. As part of our response effort, we reported the incident to the Federal Bureau of Investigation (FBI) and hired outside cyber incident response resources to assist us in restoring and verifying the security of our network and systems, and to investigate the attack. These resources successfully allowed GHC-SCW to bring our systems back online methodically and safely.

What information was involved?

On February 9, 2024, during our investigation, we discovered indications that the attacker had copied some of GHC-SCW's data, which included protected health information (PHI). The PHI that the attacker stole may have included member/patient name, address, telephone number, e-mail address, date of birth and/or death, social security number, member number, and Medicare and/or Medicaid number. Our discovery was confirmed when the attacker, a foreign ransomware gang, contacted GHC-SCW claiming responsibility for the attack and stealing our data.

What is GHC-SCW doing?

We have no indication that information has been used or further disclosed. Please be assured that we have taken additional steps to help mitigate any harm that might result from this incident by working with the FBI and U.S. Cybersecurity and Infrastructure Security Agency (CISA), informing all affected individuals, all necessary state and federal agencies, and certain consumer reporting agencies. To reduce the risk of this happening again, we have implemented enhanced security measures across all our systems and networks. This includes strengthening existing controls, data backup, user training and awareness, and other measures.

What can you do?

Please review communications from GHC-SCW and other healthcare providers, including electronic messages, billing statements, and other communications. If you notice anything that you did not authorize or services you did not receive, contact GHC-SCW immediately.

Moreover, we are offering affected individuals monitoring services for one (1) year, however we are not permitted to enroll our members directly. See the additional information included with this letter for more information about how to enroll in monitoring services. If you have questions about this incident, please call 1-800-xxx-xxxx during normal business hours.

It is your right to file a privacy complaint with the Office for Civil Rights (OCR). You can reach them by calling toll-free at (877) 696-6775, by writing to the U.S. Department of Health and Human Services, 200 Independence Avenue, S.W., Washington, D.C., 20301 or by visiting their website at https://www.hhs.gov/hipaa/filing-a-complaint/index.html. For additional guidance on steps to take to protect your personal information please visit ghcscw.com/cybersecurity/ or contact the Federal Trade Commission at www.ftc.gov/idtheft or (877) 438-4338; TTY: 1-866-653-4261.

Sincerely,

Crystal Powers

Crystal Powers
Health Information Management & Privacy Manager (Privacy Officer)
Group Health Cooperative of South Central Wisconsin

Esta carta es una notificación de infracción de su información de salud. Si desea leer esta carta en su idioma de preferencia, por favor visite nuestro sitio web: ghcscw.com/cybersecurity/.

Daim ntawv no yog sau qhia paub tias tib neeg nyiag nkag mus saib koj cov ntaub ntawv kho mob. Yog koj xav nyeem daim ntawv no sau ua koj hom lus, thov nkag mus rau peb qhov chaw saib: ghcscw.com/cybersecurity/.

هذه الرسالة عبارة عن إشعار بانتهاك معلوماتك الصحية. إذا كنت ترغب في قراءة هذه الرسالة بلغتك المفضلة، يرجى زيارة موقعنا على الإنترنت: ghcscw.com/cybersecurity/

Cyber Monitoring Services Information

In response to the incident, we are providing the parents of impacted minor dependents with access to **Cyber Monitoring** services for you and your minor child for <<ServiceLength>> at no charge. Cyber monitoring will look out for yours and your child's personal data on the dark web and alert you if your personally identifiable information or your child's is found online. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Cyber Monitoring services at no charge, please log on to **<<URL>>** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<CODE HERE>**. Once you have enrolled yourself, click on your name in the top right of your dashboard and select "Manage Family Protection" then "Add Family Member" to enroll your child. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and an email account and will require enrollment by parent or guardian first. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What if I want to speak with GHC-SCW regarding this incident?

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday. Please call 1-xxx-xxx-xxxx and supply the fraud specialist with your unique code listed above.

While call center representatives should be able to provide thorough assistance and answer most of your questions, you may still feel the need to speak with GHC-SCW regarding this incident. If so, please call GHC-SCW's Member Services department at 1-608-828-4853 or 1-800-605-4327 from 8:00 a.m. to 5:00 p.m. Central time, Monday through Friday.