HACKLEY COMMUNITY CARE
For Your Whole Life

Notification of Data Security Incident

Muskegon, MI – Hackley Community Care (HCC) has become aware of a data security incident that may have impacted personal information and protected health information belonging to certain current and former patients.

On or about September 24, 2020, HCC fell victim to a phishing attack as a phishing email containing a malicious link was sent to several HCC employees. Following an internal investigation, it was discovered that unauthorized forwarding rules had been placed on an HCC employee email account. Upon discovery, HCC performed a password reset for the affected account, immediately launched an investigation, and engaged with independent cybersecurity experts to provide assistance. As a result of this investigation, HCC learned that one (1) employee email account was accessed without authorization between September 7, 2020, and September 24, 2020, as a result of the above-referenced phishing campaign.

Upon receipt of confirmation of unauthorized access to the HCC employee email account, HCC engaged the same independent cybersecurity experts to determine whether the accessed employee email account contained personal information and/or protected health information that may have been subject to unauthorized access. On December 18, 2020, as a result of that review, HCC learned that information belonging to certain current and former patients was contained within the accessed email account. HCC worked diligently to identify contact information for all potentially affected individuals in order to provide them with notice of the incident.

The above-referenced unauthorized access was limited to the one (1) HCC email account and did not extend to other HCC information systems. Moreover, HCC is not aware of any information to suggest that any information within the affected email account was actually viewed or misused. Nonetheless, out of an abundance of caution, HCC provided notice to potentially affected individuals. HCC takes the security of all information very seriously and is implementing additional security measures to help prevent a similar occurrence in the future.

Notification letters are being sent to potentially impacted individuals whose contact information was identified. The letters include information about this incident and steps the potentially impacted individuals can take to monitor and help protect their information.

HCC has established a toll-free call center to answer questions about the incident and to address related concerns. The call center is available Monday through Friday from 8:00 a.m. to 7:00 p.m. Central Time and can be reached at 1-800-783-0373. As an additional precaution, HCC is offering complementary credit monitoring services through TransUnion to some potentially impacted individuals. HCC also notified the U.S. Health and Human Services Office for Civil Rights and consumer reporting agencies of this incident.

The privacy and protection of private information is a top priority for HCCC, and we deeply regret any inconvenience or concern this incident may cause.

The following information is provided to help individuals wanting more information about the steps that they can take to protect themselves:

What steps can I take to protect my private information?

- If you detect suspicious activity on any of your accounts, you should promptly notify the financial institution or company with which the account is maintained. You should also report any fraudulent activity or any suspected incidents of identity theft to law enforcement.

- You may obtain a copy of your credit report at no cost from each of the three nationwide credit reporting agencies. To do so, visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three agencies appears at the bottom of this page.

- Notify your financial institution immediately of any unauthorized transactions made, or new accounts opened, in your name.

- You can take steps recommended by the Federal Trade Commission to protect yourself from identify theft. The FTC's website offers helpful information at www.ftc.gov/idtheft.

How do I place a security freeze on my credit file?

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report in connection with any new credit application, which will prevent them from extending credit. A security freeze generally does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting agencies.

You should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report.

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail: 1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.); 2. Social Security Number; 3. Date of birth; 4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years; 5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed; 6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); 7. Social

Security Card, pay stub, or W-2. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

How do I obtain a copy of my credit report?

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every twelve (12) months. To do so, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three agencies is included in the notification letter and is also listed at the bottom of this page.

How do I put a fraud alert on my account?

You may consider placing a fraud alert on your credit report. This fraud alert informs creditors of possible fraudulent activity within your report and requests that creditors contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact Equifax, Experian or TransUnion and follow the Fraud Victims instructions. To place a fraud alert on your credit accounts, contact your financial institution or credit provider. Contact information for the three nationwide credit reporting agencies is listed below.

Contact information for the three nationwide credit reporting agencies is as follows:

Equifax Security Freeze	Experian Security Freeze	TransUnion (FVAD)
PO Box 105788	PO Box 9554	PO Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
1-800-685-1111	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com