CCM Health
c/o Cyberscout
1 Keystone Ave, Unit 700
Cherry Hill, NJ 08003
DB-08186b

[redacted]

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

April 3, 2024

Notice of a Data Breach

Dear [redacted]

CCM Health writes to inform you of a network security incident involving some of your individual personal and/or health information. CCM Health provides health services through public hospitals and healthcare facilities, which requires access to certain personal and/or health information. The privacy and security of the information we maintain is of the utmost importance to CCM Health. We wanted to provide you with information about the incident and let you know that we continue to take significant measures to protect your personal information.

What Happened?

CCM Health became aware of potential unauthorized access to its network.

What We Are Doing

As soon as we became aware of the issue, we launched an investigation, contained and secured the network, eradicated the threat and alerted law enforcement. As part of the investigation, we engaged third-party cybersecurity professionals experienced in handling these types of incidents. The investigation aimed to determine the nature and scope of the incident and whether any sensitive data, including personal and/or health information, was accessed and/or acquired by the unauthorized party.

After a thorough and detailed forensic investigation, we concluded the unauthorized accessed the network between April 3, 2023 and April 10, 2023, and, as a result, may have accessed and removed a number of files from our network. Upon learning this, we immediately conducted an extensive and comprehensive review of the impacted files and, on February 12, 2024, we discovered that some of the files contain your personal and/or health information. On March 28, 2024, we located your last known address to provide you with direct notice of this incident.

What Information Was Involved?

The information potentially involved your full name and Date of Birth and Medical Information. If your medical information is involved, this may include a medical record number, patient account number, prescription information, healthcare provider's name, medical diagnosis, diagnosis code, treatment type, treatment location, treatment date, admission date, discharge date, and/or lab results. This is not an exhaustive list nor can we confirm that each aforementioned data element was affected as it relates to you.

What You Can Do

To date, we are not aware of any reports of identity fraud or improper use of your personal and protected health information as a direct result of this incident. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

This letter provides precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis. To the extent that it is helpful, we are also suggesting steps you can take to protect your medical information. For more information, please review the "Other Important Information" section.

For More Information

CCM Health values your privacy and deeply regrets that this incident has occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information. Since detecting the incident, we have reviewed and revised our information security practices, and implemented additional security measures to mitigate the chance of a similar event in the future.

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, excluding holidays. Please call the help line at 1-833-966-0881.

Sincerely,

CCM Health

OTHER IMPORTANT INFORMATION

1. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348-5069
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
https://www.transunion.com/fraud-alerts
(800) 680-7289

2. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(888) 298-0045

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
(888) 397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
https://www.transunion.com/credit-freeze
(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Protecting Your Health Information.

As a general matter the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.

- Review your "explanation of benefits" statement which you receive from your health insurance company. Follow up with your insurance company or the care provider for any items you do not

recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential exposure to current date.

- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or care provider for any items you do not recognize.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.