



Capital Region[®]

MEDICAL CENTER

An Affiliate of  Health Care

1125 Madison Street, Jefferson City, MO • 573-632-5000 • www.crmc.org

March 25, 2022

VIA EMAIL

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

RE: Security Incident Notification

Dear Sir/Madam:

I am writing to notify you of a security incident experienced by Capital Region Medical Center, a healthcare provider in Missouri, involving personal information of four New Hampshire residents. CRMC experienced a cybersecurity incident on December 17, 2021 that disrupted its network systems. Immediately upon discovering the disruption, CRMC promptly disabled its network as a security measure, engaged a third-party cybersecurity firm, and initiated an investigation into the incident. Law enforcement was also notified, and on December 23, 2021, notice of the incident was provided to the public via CRMC's Facebook page and media reporting. The investigation concluded that an unauthorized third party gained access to files containing personal and health information.

Based on the investigation to date, while there is no indication that the electronic medical health record database was accessed, CRMC has determined that personal and health information relating to some patients and employees was contained in files accessible to the unauthorized third party. Such information included first and last name, date of birth, full mailing address, medical information, and health insurance information. For some individuals, Social Security numbers, and driver's license numbers may have been accessed. Once it became clear that data was exfiltrated and CRMC had identified the impacted files, the company retained a data review firm to identify personal information in the impacted files. The data review firm provided CRMC with a list of potentially impacted individuals for some of the data in late January, but contact information was available for only a limited number of those individuals. Also, CRMC needed to confirm the most current address for the impacted individuals. CRMC began searching its records and engaged another third-party company to help identify the most current address for impacted individuals to determine applicable notification requirements. It then started notifying the individuals and regulators on March 24, 2022.

Out of an abundance of caution, we intend to offer credit monitoring services to all individuals whose Social Security number or driver's license number was potentially involved in the incident. A sample of the notification letter we plan to send to the affected individual is enclosed. Please contact me by phone at (573) 632-5002 or by email at gcalvaruso@crmcc.org if you need any additional information regarding this incident.

Sincerely,

Gaspare Calvaruso
President

Notice of Data Breach

<Date>
VIA U.S. MAIL
<Name>
<Company>
<Address>
<City>, <State> <ZIP>

Dear <Name>,

The purpose of this letter is to inform you about an incident that may have exposed your personal information to unauthorized persons.

WHAT HAPPENED

On Friday, December 17, 2021, Capital Region Medical Center (CRMC) experienced a disruption to our network systems. Immediately upon discovering the disruption, CRMC promptly disabled our network as a security measure, initiated an investigation into the incident, and a third-party cybersecurity firm was engaged to assist. Law enforcement was also notified, and on December 23, 2021, notice of the incident was provided to the public. The investigation concluded that an unauthorized third party gained access to files containing personal and health information.

WHAT INFORMATION WAS INVOLVED

While there is no indication that your electronic medical health record was accessed, CRMC has determined that personal and health information relating to CRMC employees was contained in files accessible to the unauthorized third party. Such information included first and last name, date of birth, full mailing address, medical information, health insurance information, Social Security numbers, and driver's license numbers may have been accessed.

WHAT WE ARE DOING

While there is no evidence of any instances of fraud or identity theft as a result of this incident, out of an abundance of caution, CRMC is notifying you to provide additional information and resources to help protect your information. Because your Social Security number or driver's license number was involved, CRMC is offering you one year of credit monitoring at no cost. We also recommend that you review any statements that you receive from your health care provider or health insurer. If you see any medical services that you did not receive, please call the provider or insurer immediately.

CRMC takes the privacy and confidentiality of the information it maintains seriously, and deeply regrets that this incident occurred. CRMC continues to evaluate its security practices, and will continue to identify opportunities to implement additional cybersecurity measures.

WHAT YOU CAN DO

Activate your complimentary credit monitoring – To help protect you from fraud or identity theft, we are offering a one-year membership to Experian's® IdentityWorksSM at no cost. This product helps detect possible misuse of your personal information. To register, please:

- Ensure that you **enroll by: June 11, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit

- Provide your **activation code:** <code>

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at 877-288-8057 by June 11, 2022 and provide them engagement number B029089.

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can access those reports by visiting www.annualcreditreport.com or calling 1-877-322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Review your health statements – Review the statements you receive from your healthcare provider and health insurer. If you see any medical services that you did not receive, please call the provider or insurer immediately.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

Report suspicious activity – If you believe you are the victim of fraud or identity theft, file a police report and get a copy of the report to submit to your creditors and others who may require proof of a crime to clear up your records.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Equifax	Experian	TransUnion	Federal Trade Commission
P.O. Box 740241	P.O. Box 9701	P.O. Box 2000	600 Pennsylvania Ave. NW
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016	Washington, DC 20580
1-866-349-5191	1-888-397-3742	1-800-916-8800	(202) 326-2222
www.equifax.com	www.experian.com	www.transunion.com	www.ftc.gov

FOR MORE INFORMATION

Protecting the privacy of your personal information is important to us, and we regret any inconvenience this incident may cause you. Please know that we are doing everything that we can to assist and guide you through this process. Should you have any questions or concerns, please contact us by calling our dedicated toll-free helpline at 855-618-3184, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Gaspere Calvaruso
President
Capital Region Medical Center
1125 Madison St.
Jefferson City, Missouri 65101