mwe.com

David Saunders
Attorney at Law
dsaunders@mwe.com
312-803-8305

March 28, 2022

VIA PRIORITY MAIL

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Security Incident Notification

To Whom It May Concern:

We represent Charleston Area Medical Center, Inc. ("CAMC") with respect to a data security event involving the potential exposure of certain personal information of thirty-two (32) Maryland residents. CAMC is a regional not-for-profit health system with locations in West Virginia. By providing this notice, CAMC does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On January 10 and 11, 2022, an unauthorized individual accessed the email accounts of a small number of CAMC employees through an email phishing scam. Upon learning of the initial unauthorized access on January 10, 2022, CAMC immediately took steps to terminate the unauthorized access and secure the affected email accounts. CAMC also launched an internal investigation into the incident and engaged a leading cybersecurity forensics firm to perform a review of the affected email accounts. CAMC also engaged in a time-consuming review of tens of thousands of documents in the potentially affected email accounts. That email review did not conclude until March 16, 2022. CAMC's review ultimately determined that the affected email accounts contained the following types of personal information about thirty-two (32) Maryland residents: first and last name; date of birth; medical record number; and health information (e.g., discharge date, test results or other diagnostic or treatment information). A notification letter will be sent to each of these individuals on March 28, 2022 via regular mail. A copy of the template notification letter is enclosed.

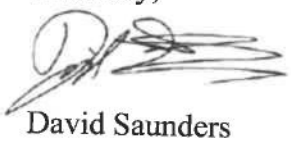
Based on its forensic investigation, CAMC believes that the unauthorized individual was interested in harvesting access credentials for CAMC employee accounts rather than accessing individuals' personal information. CAMC has no reason to believe that any of the potentially impacted personal information has or will be used for any improper purpose and there was no indication of actual data exfiltration.

Following the incident, CAMC has taken various steps to enhance its data security measures to prevent the occurrence of a similar event in the future. For example, CAMC has migrated to a new email system, which will include additional technical anti-phishing safeguards, and requires employees to use multi-factor authentication to access their email accounts on the new email system. In addition, CAMC routinely trains its workforce members on data security matters, including the importance of remaining vigilant against phishing attacks, and is planning additional training related to this incident.

CAMC takes the privacy and security of its patients' personal information seriously and, as detailed above, has taken steps designed to reduce the likelihood of a similar event occurring in the future.

If you have any questions, please contact me at dsaunders@mwe.com or (312) 803-8305.

Sincerely,



David Saunders

Enclosures

Charleston Area Medical Center

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

PRIVACY OFFICE

130-138 57th St.
Building 3, Unit 2
Charleston, WV 25304
(304) 388-1187
Fax: (304) 388-1189

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

CONSUMER PROTECTION DIVISION
RECEIVED
MAR 30 2022
OFFICE OF
THE ATTORNEY GENERAL

<<Date>>

Dear <<Name 1>>:

NOTICE OF DATA BREACH

At Charleston Area Medical Center (CAMC), we are committed to protecting the confidentiality and security of your personal information. We are sending you this letter to let you know that CAMC was recently the victim of an email phishing incident that may have resulted in unauthorized access to your personal information. *At this time, we are not aware of any misuse of your personal information.*

WHAT HAPPENED?

On January 10 and 11, 2022, an unauthorized individual accessed the email accounts of a small number of CAMC employees through an email phishing scam. Upon learning of the initial unauthorized access on January 10, 2022, we took steps to terminate the unauthorized access and secure the affected email accounts. We also investigated the incident with assistance from a leading cybersecurity forensics firm and performed an extensive review of the impacted email accounts, which was completed on March 16, 2022. Based on the available forensic evidence, we believe that the unauthorized individual was interested in collecting login information for CAMC employee accounts rather than accessing individuals' personal information. We are notifying you of this incident because your personal information was available in at least one of the affected email accounts.

WHAT INFORMATION WAS INVOLVED?

The affected CAMC employees' email accounts contained the following types of your personal information: first and last name; medical record number, and health information (e.g., discharge date, test results or other diagnostic or treatment information).

WHAT WE ARE DOING

We have enhanced our data security measures to prevent the occurrence of a similar event in the future. For example, we have migrated to a new email system, changed user accounts, and require multi-factor authentication into all mailboxes on the new email system. We also routinely train our employees on data privacy and cybersecurity issues.

WHAT YOU CAN DO

Although we have no reason to believe that your information has been, or will be, misused because of this incident, you should consider taking the following steps to protect yourself:

- Read account statements from your health care providers, explanations of benefits (EOBs) from your health plan and other documents related to medical services to make sure they do not include services you did not receive.
- Be attentive to documents related to medical services that you usually receive and that suddenly do not arrive, as you usually receive them.
- All mail related to medical or financial information should be destroyed and preferably shredded before you throw it away.

- Be careful when offering personal information over the phone, mail or internet, and unless you are sure of the person with whom you are dealing, offer as little information as possible.
- Review the "General Information About Identity Theft Protection" materials that are included with this letter. You should always remain vigilant for threats of fraud and identity theft by regularly reviewing your account statements and credit reports.

FOR MORE INFORMATION

We regret this incident and apologize for any inconvenience it may cause you. If you have any questions or concerns, please contact us toll-free by calling 1-866-995-5260, Monday through Friday, from 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely,

Debbie Boland
Privacy Officer

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Credit Reports. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. **You may contact the nationwide credit reporting agencies at:**

Equifax	**Experian**	**TransUnion**
P.O. Box 105788 Atlanta, GA 30348 www.equifax.com (800) 525-6285	P.O. Box 9554 Allen, TX 75013 www.experian.com (888) 397-3742	P.O. Box 2000 Chester, PA 19016 www.transunion.com (800) 680-7289

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Place a Security Freeze on your Credit Report. You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed at above. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. You can place a freeze and lift a security freeze on your credit report free of charge.

You may contact the Federal Trade Commission (FTC) and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the FTC and/or your state's attorney general office about for information on how to prevent or avoid identity theft. You can contact the FTC at: **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20508, www.ftc.gov, 1-877-IDTHEFT (438-4338).

For District of Columbia Residents: District of Columbia Office of the Attorney General, 400 6th St. NW, Washington, DC 20001, https://oag.dc.gov, (202) 727-3400

For Iowa Residents: State law advises you to report any suspected identity theft to law enforcement or to the Iowa Attorney General, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, 1-888-777-4590

For Maryland Residents: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023

For Massachusetts Residents: You have the right to obtain a police report if you are the victim of identity theft.

For New Mexico Residents: You have certain rights pursuant to the federal Fair Credit Reporting Act (FCRA). For more information about the FCRA, please visit www.ftc.gov

For North Carolina Residents: North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, 1-877-566-7226