NOTICE OF SECURITY INCIDENT

At Charleston Area Medical Center (CAMC), we are committed to protecting the confidentiality and security of your personal information. We are posting this notice because CAMC was recently the victim of an email phishing incident that may have resulted in unauthorized access to certain patient, personal information. *At this time, we are not aware of any misuse of the personal information potentially affected by this incident*.

WAS I AFFECTED BY THIS INCIDENT?

CAMC is in the process of providing separate, written notification to affected individuals for whom we have mailing addresses. We are posting this notice pursuant to Federal law for those individuals for whom we did not have addresses. Ordinarily, if you were a patient at CAMC, we have your address.

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, CAMC 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.

WHAT INFORMATION WAS INVOLVED?

The affected CAMC employees' email accounts contained the following types of personal information: first and last name; medical record number; and health information (e.g., discharge date, test results or other diagnostic or treatment information). In addition, for less than 0.001% of the potentially affected population, the impacted data included Social Security numbers and/or financial account numbers (but without any PIN or security access code needed to gain access to the corresponding financial account).

WHAT WE ARE DOING

We have enhanced our technical security measures to prevent the occurrence of a similar event in the future. We also routinely train our employees on data privacy and cybersecurity issues, and will be conducting additional training related to this incident.

WHAT YOU CAN DO

We encourage you to remain vigilant for threats of fraud and identity theft by regularly reviewing your account statements and credit reports. We also encourage you to read account statements from your health care providers, explanations of benefits from your health plan, and other documents related to medical services to make sure they do not include services you did not receive.

FOR MORE INFORMATION

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.