167806

Beaumont

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULY

[redacted]

[redacted]

Dear [redacted]

The privacy and security of the personal information we maintain is of the utmost importance to Beaumont Health ("Beaumont"). We are writing to inform you of a recent data security incident that we identified and addressed that may have involved some of your information. This letter provides information about the incident, explains the services we are providing to you, and explains how we help protect your information.

What Happened?

Beaumont was the target of an email phishing campaign that resulted in a limited number of employees receiving a suspicious email containing a malicious link. A small number of employees fell victim to the phishing campaign, resulting in an unauthorized individual gaining access to those employees' email accounts. Upon learning of the incident, Beaumont disabled the accessed email accounts and required mandatory password resets to prevent further misuse.

There is no evidence that the purpose of the phishing campaign was to obtain patient information and we have no evidence that any information was actually acquired or used by the unauthorized individual. However, we are providing notice out of an abundance of caution.

What We Are Doing.

Upon learning of this issue, we commenced a prompt and thorough investigation, working closely with external cybersecurity professionals. After an extensive forensic investigation and comprehensive manual document review, we discovered on March 29, 2020 that one or more of the email accounts that were accessed between May 23, 2019 to June 3, 2019 contained some of your personal and/or protected health information.

We are currently in the process of implementing additional technical safeguards on our email system to prevent the recurrence of similar incidents. We have also implemented additional training and education for our employees to increase awareness of the risks of malicious emails and to educate employees on identification and handling of malicious emails.

What Information Was Involved.

One or more of the accessed email account(s) contained some of your personal and/or protected health information, including [redacted].

What You Can Do.

We have no evidence that any of your information has been misused. However, we recommend that all patients and personal representatives of patients monitor insurance statements for any transactions related to care or services that have not actually been received. We are also including a list of steps that can be taken to help protect your medical information.

For More Information.

Please accept our apologies that this incident occurred. We have taken necessary steps to prevent this from happening again. We remain fully 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 to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable about what you can do to help protect your information. The response line is available Monday through Friday, 9:00 a.m. to 6:30 p.m. EST.

Sincerely,

Privacy Officer
Beaumont Health

Protecting Your Medical Information.

We have no evidence that your medical information involved in this incident was or will be used for any unintended purposes. However, the following practices can provide additional safeguards to protect against 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 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 access (noted above) 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 the care provider for any items you do not recognize.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.