Notice of Email Phishing Incident

Aultman Hospital ("Aultman") is committed to protecting the confidentiality and security of the information we maintain. We experienced an email phishing incident, and this notice explains the incident, measures that have been taken, and some steps patients can take in response.

We first became aware of the incident on May 7, 2024, after identifying unusual activity in an employee's email account. Upon learning of this, we secured the employee's account and launched an investigation. The investigation confirmed that this incident was limited to just one employee's email account and **did not** involve our electronic health records systems. Importantly, this incident **did not** disrupt our services or operations.

Our investigation determined that an unauthorized party gained access to the employee's email account and Sharepoint instance on May 7, 2024. While in the employee's SharePoint instance, the unauthorized party accessed certain files. In addition, we could not rule out the possibility that the unauthorized party also accessed certain emails and attachments in the employee's email account. Out of an abundance of caution, we conducted a comprehensive search of the Sharepoint files that were accessed by the unauthorized party and emails and attachments in the employee's email account that may have also been accessed as a result of this incident. Our review identified one or more files that contain some of the following information: names, medical record numbers, billing account numbers, provider names, dates of treatment, procedure information, and treatment information.

On July 5, 2024, we mailed notification letters to patients whose information may have been involved in the incident. We also established a dedicated, toll-free incident response line to answer questions that individuals may have. If an individual believes their information may have been involved and have any questions about this incident, please call 877-418-8555, Monday through Friday, between 8:00 a.m. – 5:00 p.m., Eastern Time, except for major U.S. holidays.

For patients whose information may have been involved in the incident, we recommend that they review the statements they receive from their healthcare providers and health insurance plans. If they see any services that were not received, they should contact the provider or health plan immediately.

We take this incident very seriously and sincerely regrets any concern this may cause. To help prevent something like this from happening again, we have implemented, and will continue to adopt, additional safeguards and technical security measures to further protect and monitor our systems.

Notice of Email Phishing Incident

Aultman Hospital ("Aultman") is committed to protecting the confidentiality and security of the information we maintain. We experienced an email phishing incident, and this notice explains the incident, measures that have been taken and some steps patients can take in response.

We first became aware of the incident on April 24, 2024, after phishing emails were sent from one employee's email account without their knowledge. Upon learning of this, we secured the employee's account and launched an investigation. The investigation confirmed that this incident was limited to just one employee's email account and **did not** involve our electronic health records systems. Importantly, this incident **did not** disrupt our services or operations.

Our investigation further determined that an unauthorized party accessed the Aultman employee's email account between the dates of April 22 and April 24, 2024. Although the likely purpose of the unauthorized access to the employee's email account was to perpetrate a phishing email scheme, the investigation cannot rule out the possibility that the unauthorized party accessed emails and attachments in the employee's email account. Therefore, out of an abundance of caution, Aultman is conducting a manual review of the contents of the employee's mailbox. Through our ongoing review, we identified emails and attachments that contain patient information, including patient names and medical record numbers. These emails and attachments also may contain dates of birth, addresses, patient account numbers, health insurance identification numbers, diagnoses and/or treatment information.

On June 21, 2024, we began mailing letters to patients whose information may have been involved in the incident. We also established a dedicated, toll-free incident response line to answer questions that individuals may have. If an individual believes their information may have been involved and have any questions about this incident, please call 800-482-2349, Monday through Friday, between 8:00 a.m. – 5:00 p.m., Eastern Time, except for major U.S. holidays.

For patients whose information may have been involved in the incident, we recommend that they review the statements they receive from their healthcare providers and health insurance plans. If they see any services that were not received, they should contact the provider or health plan immediately.

We take this incident very seriously and sincerely regret any concern this may cause. To help prevent something like this from happening again, we have increased cybersecurity training and implemented additional safeguards and technical security measures to further protect and monitor our systems.