



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 after phishing emails were sent from one employee’s email account without their knowledge on April 24, 2024. 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.

On October 1, 2024, Aultman completed its investigation. Our investigation determined that an unauthorized party accessed the Aultman employee’s email account between the dates of April 22, 2024 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 conducted a manual review of the contents of the employee’s mailbox. Through our 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. For some patients, the emails and attachments contained their Social Security numbers.

Between June 21, 2024 and October 23, 2024, we mailed letters to patients whose information may have been involved in the incident. Complimentary credit monitoring is being offered to patients whose Social Security and/or driver’s license numbers may have been involved. 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 implemented additional safeguards and technical security measures to further protect and monitor our systems.