

Substitute Notice

Notice to our Patients About an Email Phishing Incident

Legacy Community Health Services (“Legacy”) is committed to protecting the confidentiality of our patients’ information. Regrettably, this notice is to inform our patients of a recent incident that may have involved some of that information.

On July 29, 2020, we learned that an employee responded to a phishing email on July 28, 2020, believing it to be legitimate. We immediately secured the account, began an investigation, and worked with a computer forensic firm to better understand the incident and what information may have been accessible to the unauthorized person.

We have no evidence that anyone’s personal information was actually viewed by the unauthorized person. However, in an abundance of caution, we reviewed all of the emails and attachments that may have been accessible to the unauthorized person. We found that this information included some patient names, dates of service, and health information related to care at Legacy. In limited instances, the email account also included patient Social Security numbers; however, financial account and payment information was not included. Again, we have no reason to believe that the unauthorized person viewed or misused any patient information.

We began mailing letters to affected patients on September 25, 2020 and established a dedicated and confidential call center for patients to call with questions. If you believe you are affected by this incident, please call 1-888-490-0839, Monday through Friday, 8:00 a.m. to 8:00 p.m., Central Time.

We recommend that our patients review the statements they receive from their healthcare providers. If they see services they did not receive, please contact the provider immediately. For those patients whose Social Security numbers were included in the email account, we are offering a complimentary membership of credit monitoring and identity protection services.

We take the privacy and confidentiality of our patients’ information very seriously, and deeply regret any inconvenience or concern this incident may cause our patients. To help prevent something like this from happening again, we are enhancing our email security and reinforcing education with our employees on how to identify and avoid phishing emails.