Substitute Notice

Notice to our Patients About an Email Phishing Incident

Legacy Community Health Services ("Legacy") is committed to protecting the confidentiality and security of our patients' information. Regrettably, this notice is about an email phishing incident we are currently looking into that may have involved some of that information. A phishing email is an email sent from someone pretending to be from someone else to get personal information.

On April 16, 2020, we learned that a Legacy employee responded to a phishing email believing it to be legitimate. We immediately secured the account and began an investigation. A computer forensic firm was engaged to investigate the scope of the incident and determined that an unauthorized person accessed the email account between April 10, 2020 and April 16, 2020. We are in the process of thoroughly reviewing the contents of the email account to identify those patients whose information may have been accessible to the unauthorized person. We expect that some patient information is contained in the email account, including patient names, dates of service, and health information related to their care at Legacy. We will update this notice as we obtain more information.

We are continuing to investigate this incident and anticipate notifying patients in the coming weeks. Although we have no reason to believe that any patient information has been misused, out of an abundance of caution, we have set up a dedicated and confidential call center for patients to call with questions. If you have questions about this incident, please call 1--833-613-0919, Monday through Friday, 8:00 a.m. to 6:00 p.m. Central Time. We recommend that patients review the statements they receive from their healthcare provider. If they see services they did not receive, please contact the provider immediately.

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 in the process of enhancing email security on all email accounts and we are reinforcing education with our employees on how to identify and avoid phishing emails.