

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 enhancing our email security, have enabled multi-factor authentication on all email accounts, and we are reinforcing education with our employees on how to identify and avoid phishing emails.

Aviso a nuestros pacientes sobre un incidente de correo electrónico fraudulento (phishing)

En Legacy Community Health Services (“Legacy”) tenemos el compromiso de proteger la confidencialidad y la seguridad de la información de nuestros pacientes. Lamentablemente, este aviso trata sobre un incidente de phishing por medio de correo electrónico que estamos tratando actualmente y que puede haber incluido algo de esa información. Un correo electrónico de phishing es un correo electrónico fraudulento, enviado por alguien que pretende ser otra persona con el fin de obtener información personal.

El 16 de abril de 2020 nos enteramos que un empleado de Legacy respondió a un correo electrónico fraudulento creyendo que era legítimo. Inmediatamente aseguramos la cuenta del empleado e iniciamos una investigación. Se contrató a una empresa de informática forense para investigar el alcance de este incidente, y se determinó que una persona no autorizada accedió la cuenta de correo electrónico entre el 10 y el 16 de abril de 2020. Actualmente estamos en proceso de revisar minuciosamente el contenido de la cuenta de correo electrónico para identificar a los pacientes cuya información pudo haber estado accesible a la persona no autorizada. Se espera que la cuenta de correo electrónico haya contenido algo de información de pacientes, incluyendo nombres de pacientes, fechas de servicio e información de salud relacionada con los servicios recibidos en Legacy. Actualizaremos este aviso conforme vayamos obteniendo más información.

Continuamos investigando este incidente y anticipamos notificar a los pacientes en las próximas semanas. Aunque no tenemos motivos para pensar que la información de pacientes haya sido utilizada indebidamente, como una medida extrema de precaución hemos creado un centro de llamadas específico y confidencial para que los pacientes puedan llamar si tienen alguna pregunta. Si usted tiene preguntas sobre este incidente, comuníquese al 1-XXX-XXX-XXXX de lunes a viernes, de 8:00 a.m. a 6:00 p.m. Horario Central. Recomendamos a nuestros pacientes que revisen los estados de cuenta que reciban de su proveedor de atención a la salud. Si ven algún servicio que no hayan recibido, comuníquese de inmediato con su proveedor de salud.

Tomamos muy seriamente la privacidad y confidencialidad de la información de nuestros pacientes, y lamentamos profundamente cualquier inconveniencia o preocupación que este incidente pueda ocasionar a nuestros pacientes. Con el fin de evitar que esto suceda nuevamente, estamos reforzando la seguridad de nuestro correo electrónico hemos establecido un sistema de autenticación múltiple en todas nuestras cuentas de correo electrónico y estamos reforzando la educación que recibe nuestro personal acerca de cómo identificar y evitar correos electrónicos fraudulentos (phishing).

