Notice of Data Security Incident

Barlow Respiratory Hospital is committed to protecting the security and privacy of our patient information. On December 30, 2021, we began mailing notification letters to some of our patients whose information may have been involved in a data security incident.

We identified and addressed a data security incident that disrupted the operations of some of our IT systems. The incident was first identified on August 27, 2021, and in response, we immediately took steps to secure our systems, launched an investigation with the assistance of a third-party forensic investigator, and notified law enforcement. The investigation determined that an unauthorized party gained access to our systems from August 21, 2021 to September 1, 2021. The investigation also determined that the unauthorized party removed some files from our systems. In order to determine what data was involved, we conducted a review of those files.

On November 30, 2021, our review and analysis of the files involved in the incident determined that they contained certain information for some of our patients, including names, contact information, dates of birth, Social Security numbers, driver's license numbers, medical record numbers, treatment information, diagnosis information, dates of service, provider names, financial account information and/or health insurance information.

In an abundance of caution, we encourage our patients who were notified about the incident to enroll in the complimentary credit monitoring services we are offering. Barlow patients should also review the statements they receive from their healthcare providers and health insurance plans, and contact their providers or health plans immediately if they see services that were not received. Additionally, we encourage our patients to remain vigilant to the possibility of fraud by reviewing their financial account statements and immediately reporting any suspicious activity to their financial institution.

Barlow Respiratory Hospital takes this incident very seriously and we 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. A dedicated call center has been established to answer questions about this incident, which can be reached at 1-833-608-3027, Monday through Friday, between 6:00 am and 6:00 pm Pacific Time.