HIPAA

Monthly Alert

JULY 2019

According to the breach summary posted on the Department of Health and Human Services' Office for Civil Rights breach portal, a private practice experienced a data breach that impacted more than 23,300 patients.

On November 23, 2018, an email account breach was detected by the private practice when suspicious activity was detected related to an employee's email account. The account appeared to have been used to send phishing emails to individuals in the employee's contact list. Those emails attempted to convince the recipients to make fraudulent payments. The private practice took action and locked the hacker out of the account to secure the entire email environment. Also, all users were required to set new, complex passwords. The practice hired a third-party computer forensics firm to investigate the attack and determine the scale of the breach. In conclusion to the investigation on December 14, 2018, it was revealed that the attacker had gained access to multiple email accounts from August 14 to November 23, 2018. The breach was determined to be limited to the email system, and the medical record system was unaffected.

If you have any suspicions that your e-mail account has been hacked, call Liberty's Security Officer Eli Back: 610-668-8800 extension # 183.

Analysis of the compromised email accounts revealed they contained electronic personal health information (PHI).

In addition to patients' names, the following information was potentially compromised: addresses, email addresses, phone numbers, dates of birth, dates of service, diagnoses, medical conditions, lab test results, information related to diagnostic studies, treatment information, insurance information, and, for some patients, costs of medical services, social security numbers, and driver's license numbers.

Following the incident, implemented protections for phishing attacks were enhanced.

The practice modified how authorized individuals accessed the network and the IT Department's computing environment. Additional mandatory security awareness training was also provided to the entire workforce.

Better to be safe than sorry.

For any cyber-security questions, contact Liberty's Security Officer Eli Back: 610-668-8800 ext. 183.

Reference

https://www.hipaajournal.com/23300-patients-affected-by-critical-care-pulmonary-sleep-associates-email-hack/

Please look for next month's HIPAA alert delivered through your email.
You can also find the HIPAA monthly alerts on Employee Self Service (ESS).

Should you have any questions regarding this alert please contact: Judith Ann Shields
Email: judith.shields@libertyhealth.com | Phone: 610.668.8800 ext.193

Liberty Healthcare Corporation
THE FREEDOM TO SUCCEED™