Health Information Compliance Alert

Review the Top 3 Biggest Breaches this Summer

Hint: Teach your staff about the dangers of phishing.

June, July, and August are traditionally steamy, but no one could have predicted that data breaches would be off the charts, too. With over 3.2 million individuals' protected health information (PHI) impacted, the summer of 2018 put HIPAA in the hot seat.

Take a look at these three massive breaches:

1. Phishing part 1: Iowa Health System, which does business as **UnityPoint Health**, felt the sting of social engineers, suggests the July 31 Office for Civil Rights (OCR) breach portal data. Between March and April of 2018, employees at UnityPoint Health fell victim to phishing ploys through email, declared the organization's notice of breach. "Some of the compromised accounts included emails or attachments to emails, such as standard reports related to healthcare operations, containing protected health information [PHI] and/or personal information for certain patients," the notification stated.

According to the UnityHealth release, the organization believes - pointing to outside resources and forensic evidence - that the hackers have not tried to "misuse" any of the 1,421,107 individuals' ePHI. The group, instead, insists the phishers attacked the email system in hopes of gaining financial information "rather than on obtaining patient information," reveals the UnityHealth bulletin.

Read the UnityHealth breach notice at www.unitypoint.org/filesimages/About/Security Substitute Notification.pdf.

2. Phishing part 2: Back in September 2017, the **Augusta University (AU) Medical Center, Inc.** in Georgia uncovered some phishy emails, which then led the healthcare provider to investigate, maintained the organization's notice. "On July 31, 2018, investigators determined that email accounts accessed earlier by an unauthorized user may have given them access to the personal and protected health information [PHI] of approximately 417,000 individuals," explained the breach notification.

Unfortunately, a plethora of sensitive patient data was exposed in the hack, which included "addresses, dates of birth, medical record numbers, medical information, treatment information, surgical information, diagnoses, lab results, medications, dates of service and/or insurance information," AU Medical Center said. Social Security numbers and drivers license information may have also been compromised.

Review the AU Medical Center phishing attack at www.augusta.edu/notice/?campaign_url=https://www.augustahealth.org/&ga_cid=2142552651.1534519563#notice.

3. Disposal debacle: In the midst of a hospital demolition, Jefferson City, Missouri's **SSM Health St. Mary's Hospital** unearthed "documents and other materials containing patient information" hidden in a remote section of the "former hospital campus," noted an SSM Health notification on the breach.

Though "SSM Health feels that this incident does not represent a significant risk to patients," the organization is still following HIPAA compliance and procedures, the notice mentioned. According to the OCR breath portal data, 301,000 individuals were affected by the breach.

See the SSM Health story at www.ssmhealth.com/newsroom/2018/7/notice-of-medical-information-discovered.