Health Information Compliance Alert

Compliance: Check Out the Mid-Year HIPAA Breach Numbers

Tip: Ensure BAs have a handle on compliance.

If you were just starting to get back into a groove at your practice, you may want to add HIPAA compliance to your staff training to-do list. The HHS Office for Civil Rights (OCR) breach portal statistics suggest 2021 is going to be a banner year - and cybersecurity incidents are on the rise.

Background: Though last year's numbers were skewed due to COVID-19, the first half of 2020 saw only 133 HIPAA breaches with hacking/IT incident as the top root cause. In 2021, a whopping 325 HIPAA breaches occurred from Jan. 1 to July 4, and hacking again was the overarching culprit. The five biggest breaches, which impacted millions of individuals' protected health information (PHI), were the result of hacking or an IT incident with three designated as network server issues, one caused by an email infiltration, and one listed as "other."

Here's the lowdown on the three largest PHI violations:

1. Florida part 1: Tallahassee-based Florida Healthy Kids Corporation (FHKC), a nonprofit children's' health insurance provider, discovered that a data breach had occurred through its web hosting vendor, Jelly Bean Communications Design, LLC. FHKC found out about the incident on Dec. 9, 2020, and the health plan employed an expert cybersecurity team to investigate the breach.

"Significant vulnerabilities" were identified on the hosting platform and in the "databases that support the online Florida KidCare application," an FHKC release says. The cybersecurity inquiry also revealed that "these vulnerabilities spanned a seven-year period from November 2013 until December 2020," notes the release.

On Jan. 29, the OCR breach portal indicated that 3.5 million individuals' PHI was affected in the FHKC cyber attack.

2. Florida part 2: The larger of the two business associate (BA) breaches in May happened at Ft. Lauderdale-based 20/20 Eye Care Network, Inc. and impacted 3,253,822 individuals PHI. "Insider wrongdoing" is listed as the type of breach, which occurred between Jan. 11, 2021 and Feb. 18, 2021, according to the incident report filed with Maine's Attorney General by the BA.

Names, other personal identifiers, and Social Security numbers may have been compromised in the massive breach, the Maine report indicates.

3. Texas: NEC Networks, LLC, d/b/a CaptureRx based in San Antonio was the victim of a ransomware attack, according to a notification from the firm. CaptureRx assists healthcare providers in dealing with 340B administrative burdens, the vendor's website says.

CaptureRx began seeing unusual activity in February 2021, and the breach was discovered on March 30, 2021, maintains the IT vendor's filing with the Maine Attorney General. The OCR added the incident to its breach portal on May 5, highlighting that 1,656,569 individuals had their PHI usurped.

Consider These Other Breach Stats

Network server issues remained a major thorn in the sides of covered entities (CEs) across the board with 175 breaches

thus far in 2021.

"The reason we're seeing 'network server' next to so many breaches is because that's where large amounts of PHI data is stored - on a server that is located within the organization's network, in a database or file share," advises **Jen Stone, MCIS, CISSP, CISA, QSA**, principal security analyst with Security Metrics in Orem, Utah.

Another reason network servers are vulnerable to cyber attacks is due to the amount of information organizations store on them, Stone cautions. "Network servers are great targets for hackers because they can count on stealing a lot of information at one time from a server, while there might only be a subset of that information on a laptop, and only a few records in an email."

Take a look at this breakdown of the mid-year breach totals collated from the OCR breach portal:

HIPAA Breach Investigation Statistics From Jan. 1, 2021 to July 4, 2021

Resource: Find more breach investigation data at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.