Health Information Compliance Alert

Case Study: Summer Breaches Pummel Providers

Cyber attack tops the list of reasons for the uptick in PHI losses.

If your practice is preparing for an end-of-year compliance check, you may want to add health IT to your to-do list. Federal reports indicate that this summer was a virtual hackathon of health organizations' emails and networks, impacting millions of patients' protected health information (PHI).

Reminder: The HHS Office for Civil Rights (OCR) breach portal reports on HIPAA breaches that impact 500 individuals or more, which is required of the HHS Secretary by section 13402 (e)(4) of the Health Information Technology for Economic and Clinical Health (HITECH) Act. According to evidence on the OCR's "wall of shame," hackers seemed to really double down on healthcare organizations over the summer months.

Between June and August of 2018, there were 90 breaches that included the loss of 3.2 million individuals' PHI or electronic PHI (ePHI), show the latest statistics from the breach portal. These numbers are significantly higher than last year's statistics for the same time period. Over the same three months in 2017, there were only 54 breaches affecting 1,471,296 people, the OCR data reveals.

Here's a quick look at the stats:

June-August 2018: HIPAA Breaches Affecting 500 or More Individuals

Beware of These Top Breach Issues

The OCR has not addressed the summer onslaught of breaches, but the data shows that cyber attacks accounted for a majority of the ePHI losses. Even small practices can impede hackers with thoughtful HIPAA protocols, but the initial task of creating resources and office compliance codes can be daunting. And more often than not, providers and organizations don't fully understand the federal and state rules and regulations - or the consequences.

"Well-intentioned security mistakes are dime-a-dozen," reminds **Frank Knobbe, QSA**, partner with **LBMC Information Security, LLC,** in the Nashville office in a blog post. "Often, organizations don't realize that a security specification has evolved - and rendered their current measures out-of-date."

He advises, "All too frequently, organizations simply misunderstand the standards, apply the wrong solution, and move forward blissfully unaware that they're out of compliance. The sad fact is that no amount of good intentions can protect vulnerable data."

Nuts and bolts: According to the OCR breach portal guidance, hacking was the principal culprit for loss of patients' data. Unauthorized access and disclosure ranked second with theft, loss, and improper disposal also making an impact. Here is an overview of the summer breach issues:

- **June 2018:** Unauthorized access and disclosure of networks, email systems, and paper or media were the cause of 15 of the large-scale reported breaches in June, according to the OCR. Email or network server infiltrations induced by hackers were attributed to 13 of the data breaches while six incidents were caused by theft.
- **July 2018:** Five different types of data breaches occurred in July, but hacking prompted 20 alone. One of the email hacking incidents contributed to the greatest loss of ePHI in 2018 so far with over 1.4 million affected (See story on p. 68). Other data infractions included eight unauthorized access and disclosure issues, two thefts, two incidents of materials being improperly disposed of, and one breach of a lost device.

- **August 2018:** Last month, 13 HIPAA violations were reported for hacking as opposed to eight for unauthorized access and disclosure. Two incidents of theft and one of device loss rounded out the 24 data breaches in August.

Remember, not every data breach translates into OCR enforcement. In fact, many organizations have robust risk management plans that address data breaches from the get-go. More importantly, settlements show that keeping HIPAA compliance and the federal standards in mind can greatly reduce the punishments.

Consider this: Though clinicians may be reluctant to earmark funds for data security, this recent spat of breaches highlights the critical need to invest in risk planning. Of the 90 cases over the last three months, 70 of the covered entities experiencing a major breach were healthcare providers.

Tip: "Covered entities and business associates must insulate their businesses with a comprehensive compliance plan and risk analysis addressing and mitigating any applicable privacy and security risks," advises attorney **John E. Morrone**, a partner at **Frier Levitt Attorneys at Law** in New York City.

Morrone warns, "OCR has demonstrated its propensity to impose significant fines on entities that fail to implement appropriate safeguards, independent of the number of affected individuals or the content of the protected health information included in a particular breach."

Resource: Review the breach activity at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.