Health Information Compliance Alert

Policies & Procedures: Smarten Up Your Data Retention Policy -- Pronto

Beware: Old data left on your network server will only worsen breach fallout.

Did you know that your data retention and data purging policies (or lack thereof) could put you at risk for larger and thus more expensive HIPAA breaches? Here's yet another hidden trap in the world of hacking-related breach incidents.

Background: On July 17, **University of California Los Angeles Health** (UCLA Health) reported a breach involving a hacking incident of its network server that exposed the protected health information (PHI) of 4.5 million patients. Hackers accessed parts of UCLA Health's network that contained patients' personal information, including names, addresses, birthdates, Social Security numbers, medical record numbers, Medicare or health plan ID numbers, medical conditions, medications, procedures, and test results.

Brace Yourself: Lawsuit Filings are Getting Faster

And in perhaps record time (just four days later), UCLA Health became a defendant in a class action lawsuit resulting from the breach. Filed in California federal court, the complaint alleges several violations, including violation of California's Confidential Medical Information Act, according to a July 23 analysis in The National Law Review by attorney **Jordan T. Cohen** of **Mintz Levin**.

The plaintiffs claim that the breach was a direct result of UCLA Health's failure to take "basic steps" to safeguard sensitive information, such as encryption of patient data, Cohen said. "However, it is unclear at this point the role that encryption would have played in preventing such an attack. If the hackers obtained access to UCLA's internal network, it is possible that the data would have been accessible regardless of whether it was encrypted."

Don't Make This Costly Data-Storage Mistake

What's more: Early reports of the hacking incident, which began in September 2014, indicated that hackers may have gained access to information dating back to the 1990s, said **Mark Burnette, CPA, CISSP, CISM**, a partner with **LBMC Information Security**, in a July 22 blog posting. "The question that must be asked is: why was so much older data so easily accessed in the first place?"

"It is hard to fathom a compelling reason why data sensitive PHI at that from the 1990s should still be accessible on a network," Burnette lamented. "It comes down to the fact that far too many organizations lack a data retention policy and/or data purging process."

Best practice: You should transfer older data to magnetic tapes because archived data is nearly impossible for hackers to access since it is no longer on your network, Burnette stated. The UCLA Health breach occurred because data that the organization should have archived was not "instead, it was data that was still active and accessible on network systems."

You should have a retention policy that takes into account legally mandated terms for data preservation, Burnette advised. Don't use an active computer network as long-term data storage, and "it is downright irresponsible to keep data on the network indefinitely." And when you don't need to retain data any longer, you must have a data purging policy in place for securely getting rid of old data.