COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 19, Number 4. April 10, 2019 Despite OCR Enforcement Pass, UCLA Agrees To $7.5M-Plus Settlement For 2015 Data Breach

By Theresa Defino

Just one week after the University of California Los Angeles Health Systems reported in July 2015 that hackers had infiltrated its health networks, gaining access to the protected health information (PHI) of 4.5 million current and former patients, the first class action litigation against UCLA was filed on behalf of the owner of a tapas restaurant and bar.

Ultimately UCLA Health faced 17 separate suits brought by 22 plaintiffs, none of whom showed—or were required to—that they had suffered harm from the breach.

UCLA Health still maintains there has been no evidence of data misuse. Nevertheless, last month, a California Superior Court judge gave preliminary approval to a settlement agreement to resolve the now-consolidated suits that calls for, among other things, UCLA Health to offer two years of credit monitoring and to spend "at least" $5.5 million in "new money" to enhance the cybersecurity of its data. Attorneys for the affected patients are expected to be paid $3.41 million in fees and expenses when final approval of the settlement occurs in June.

Worth noting: UCLA Health escaped enforcement action by the HHS Office for Civil Rights (OCR) for its breach. This stands apart from another recent settlement involving Anthem Inc. for $16 million *and* which was part of a $115 class action settlement ("OCR Exacts Its Pound of Flesh From Anthem With $16 Million Settlement, Corrective Actions," *RPP* 18, no. 11).

Although the breach is widely thought of as having occurred in 2015, like many others before it, the year refers to when it was announced, not when it actually began. A review of the court documents in the case reveal details of a timeline from the fall of 2014 to the summer of 2015 when breach notification was made, a period punctuated by a series of discoveries that at first seemed reassuring but later made public notice inescapable.

The information may prove valuable to other organizations, as all that suspect they have a reportable breach need to make an assessment about whether to make formal notification to OCR and the public. That process is supposed to take only 60 days, by law, but as UCLA Health's experience shows, arriving at a notification decision takes time. Additional days beyond the two months are permissible when law enforcement agencies are involved.

Hacker Activity Was Tracked

UCLA Health's investigation began Oct. 16, 2014. That was the day on which information technology staff "received alerts suggesting suspicious activity and took immediate steps to stop the suspicious activity. It then opened an investigation with the support of an information security and forensics firm and notified the FBI."

Before going public, investigators monitored UCLA Health's systems "for signs of attacker activity, with an eye toward searching for evidence of any unauthorized access or acquisition of sensitive information," including PHI. "Where signs of attacker activity were found, forensic analysis was performed including, as appropriate, installation of an advanced malware detection agent, use of a leading forensics agent, and the imaging of systems," the settlement agreement states.

Investigators were looking "specifically" for signs that hackers had gained access to the electronic health record system (EHR). To do this, they, "among other things…analyzed audit logs for the EHR, which record each time a patient record is accessed. The logs revealed no unexplained increase in the normal amount of expected traffic in the database."

While the situation may have looked good up to that point, "in early May 2015, the investigation team learned that the cyber attackers had accessed a set of servers called a `SQL cluster.' One of the databases on the SQL cluster contained information of more than 4 million current and former UCLA Health patients." Still, the "investigation team found no evidence showing that the cyber attackers accessed data in this database," but they could not determine "conclusively which (if any) databases within the SQL cluster had been accessed by the cyber attackers."

At some point, investigators "also learned that some data had been exfiltrated from the system," a transfer of "less than two gigabytes." However, this development triggered more concern because investigators discovered "the third-party logging software had an unknown error that meant it was not reliably capturing data flows out of the UCLA Health environment."

As the settlement details, this error "was corrected with an update provided by the vendor. Even if the software had been working properly," it was of limited use because "if the software had been working properly, it would not have provided information on the type of data that was exfiltrated (it only logged data volume and timing information)."

The moment of truth arrived in early June. "On June 5, 2015, following an analysis of the facts, UCLA Health made the determination that, even though it did not have evidence the attacker actually accessed or acquired personal or medical information maintained on the part of the UCLA Health network impacted by the attack, it could not conclusively rule out that possibility, and therefore providing notice of the incident was appropriate," the documents state.