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.

Suit Alleged Multiple Violations

Ultimately, it was concluded the attack may have begun Sept. 1, 2014. On July 15, 2015, nearly a year from that date, public breach notification was made.

"To reduce risk, UCLA Health is offering all potentially affected individuals 12 months of identity theft recovery and restoration services as well as additional health care identity protection tools. In addition, individuals whose Social Security number or Medicare identification number was stored on the affected parts of the network will receive 12 months of credit monitoring," officials said at the time.

The filing of a potential class action suit followed swiftly: Sirine Adlouni, who once operated a tapas restaurant, brought a case against UCLA on July 24, 2015. She is one of 21 plaintiffs who will receive $750 for their part in the suit; one individual who participated to a greater degree will receive $1,500.

Their suit alleged "violations of California's Confidentiality of Medical Information Act, Consumer Unfair Competition Law, Customer Records Act, Information Practices Act, as well as negligence, gross negligence, negligence per se, invasion of privacy, constructive fraud, conversion, bailment, unjust enrichment, breach of express contract, breach of implied contract, and breach of confidentiality."

Media reports referred to the settlement as having a value of $7.5 million, an amount Jeff Westerman, lead plaintiffs' attorney, said is a minimum that could grow depending on a number of factors and that does not reflect all possible services and payments.

Credit monitoring is just one of three benefits the settlement makes available to affected patients; it is joined by two funds that could provide reimbursements to them as well.

It remains to be seen how many individuals sign up for the identity theft protection that includes credit monitoring, which had a relatively small fraction of takers the first time it was offered. At the time of the breach, UCLA made one year of services available through an identity theft protection package. Of the 4.5 million affected individuals, just 219,000 people enrolled. An eight-month period for sign-up was permitted.

Preventive, Unreimbursed Costs May Be Covered

Sign-ups as part of the new settlement are in effect until September, but claims for reimbursement related to unauthorized use of the data at issue would be permitted for two years from the effective date of the settlement.

Experts in the case estimated that "about 175,000 people could sign up based on their experience in other cases and the notice program [called for in the settlement]. With a retail value of $239 per person [multiplied by] 175,000 people, that would be over a $42 million benefit to the class," Westerman argued in the court documents. "This anticipated sign-up value in itself demonstrates the settlement is fair, reasonable and adequate."

The settlement also establishes a "preventive measures claims" fund that would pay up to $5,000 per person to help individuals who may not have originally signed up for credit services or who do so under the new agreement and had faced costs to protect themselves from the time the breach was first announced.

An "unreimbursed loss fund [that] provides for reimbursement for identity theft incidents which occurred while settlement class members were not covered by an identity theft protection package" was also established. Amounts are capped at $20,000 per individual, while the unreimbursed loss fund itself would total $2 million.

RPP asked Westerman about the value of the settlement for the health care compliance community.

"I think cases like this and their resolution point out that [they] should audit their security and take steps to protect patient data sooner rather than later," he says. "Even if it is impossible to prevent attacks or advanced persistent threats, it is better to heighten protection in advance than pay to defend litigation, leave patient data at risk, and still have to pay for security remediation any way."

Westerman says the dollar amounts for each part of the settlement were the product of negotiation.

"Both sides had their strong views and we used an experience mediator that made a recommendation to the parties on how to bridge their differences," he tells *RPP.*

In a joint announcement issued March 21, the plaintiffs and UCLA Health said they were settling "to avoid the expense of further litigation and to provide benefits to the individuals whose information was maintained in UCLA Health's computer network."

UCLA Health noted that it "admits no wrongdoing," and "maintains that it was not liable for the cyber attack and that, following an extensive investigation, there continues to be no evidence that the cyber attackers actually accessed or acquired personal or medical information."

The organization also noted that it was subject to "hundreds of thousands of attempted attacks each year," and that it is "impossible for any institution, company, or entity to ensure that its network will be safe against each and every cyberattack."

Attorneys for UCLA Health declined to comment to*RPP* about the settlement.

Enhancements Redacted in Settlement

Although it agreed to settle, UCLA Health nevertheless defended itself in court filings, stating that the patients who sued "faced an uphill battle in this case to establish liability and the right to any relief—they would not get monetary relief because they have no unreimbursed losses due to identity theft (and statutory damages are unavailable), and they would not get an injunction compelling any security practice or policy changes because UCLA Health has voluntarily undertaken (and largely completed) substantial efforts that has further increased its data security posture."

It also pointed out that a "lack of evidence of harm connected to the cyberattack would serve as a serious impediment" to successful litigation and questioned whether the patients who brought the suit could be legally certified as a class.

However, UCLA Health did make the $5.5 million minimum commitment to upgrade its security. Like the Anthem settlement, specific expenditures are included as part of a "highly confidential" exhibit, but they are mostly redacted.

The investment in security enhancements, which could cost as much as $7.5 million, will be used to "expedite cybersecurity enhancements for the UCLA Health network," providing for the services of "six individuals, either contractors or new employees, acquisition of hardware, use of a third-party vendor, and upgrades or replacement of infrastructure," according to unredacted portions of the settlement.

OCR Was Satisfied

As noted earlier, UCLA Health's lack of enforcement by OCR doesn't inure an organization from a class action suit, demonstrating such litigation can happen independent of federal (and state) action.

OCR's $16 million settlement with Anthem helped OCR reach a record year in enforcement settlements, bringing in a total of $28.7 million ("OCR Piggybacks on Another Calif. Settlement, Adds $3M From Cottage Health to 2018 Total," *RPP* 19, no. 3). But of the 11 settlements OCR inked in 2018, one with UCLA was not among them.

The agency does not provide any detail on cases that are not subject to settlement agreements, but one way to ascertain what happens in the wake of a breach is to review entries on the agency's breach notification portal. Covered entities (CEs) and business associates (BAs) are required to report breaches affecting 500 or more individuals to OCR, which posts them on the portal. In some instances when a case is closed without formal enforcement action, OCR posts information on the portal regarding efforts at remediation that the CE or BA took.

In this case, OCR reported the following: "A hacker accessed parts of [UCLA's] computer network that contained the clinical and demographic information of approximately 4,500,000 individuals. The CE reported the incident to the Federal Bureau of Investigation and conducted a forensic analysis of the incident. The CE provided breach notification to HHS, affected individuals, and the media, and also posted substitute notice. Following the breach, the CE implemented technical and administrative safeguards designed to help detect and contain any future cyber-attacks. OCR obtained assurances that the CE implemented the corrective actions above."

Eight years earlier, however, UCLA was on the hook with OCR. In July 2011, UCLA settled with OCR for $865,000 and agreed to implement a two-year corrective action plan for instances in 2005 and 2008 involving employees who "repeatedly and without permissible reason looked at the electronic protected health information of these patients," who were celebrities.

For more information on the new settlement, see https://www.uclahealthcybersettlement.com/en. Contact Westerman at jwesterman@jswlegal.com. ✧