# Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating

The Hollywood Presbyterian Medical Center in 2004. The hospital was recently the target of a ransomware extortion plot in which hackers seized control its computer systems and then demanded that directors pay in bitcoin to regain access.

(Ricardo DeAratanha / Los Angeles Times)

[Richard Winton](http://www.latimes.com/la-bio-richard-winton-staff.html#nt=byline)Contact Reporter

Hollywood Presbyterian Medical Center paid a $17,000 ransom in bitcoin to a hacker who seized control of the hospital's computer systems and would give back access only when the money was paid, the hospital's chief executive said Wednesday.

The assault on Hollywood Presbyterian occurred Feb. 5, when hackers using malware infected the institution's computers, preventing hospital staff from being able to communicate from those devices, said Chief Executive Allen Stefanek.

**[Join the conversation on Facebook >>](https://www.facebook.com/latimes%22%20%5Ct%20%22_blank)**

“The malware locks systems by encrypting files and demanding ransom to obtain the decryption key. The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key,” Stefanek said. “In the best interest of restoring normal operations, we did this.”

The hospital said it alerted authorities and was able to regain control of all its computer systems by Monday, with the assistance of technology experts.

Stefanek said patient care was never compromised, nor were hospital records.

Top hospital officials called the [Los Angeles Police Department](http://www.latimes.com/topic/crime-law-justice/law-enforcement/los-angeles-police-department-ORGOV000939-topic.html) last week, according to police Lt. John Jenal.

Laura Eimiller, an FBI spokeswoman, said the bureau has taken over the hacking investigation but declined to discuss specifics of the case. Law enforcement sources told The Times that the hospital paid the ransom before reaching out to law enforcement for assistance.

The attack forced the hospital to return to pen and paper for its record-keeping.

Phil Lieberman, a cybersecurity expert, said that, while ransomware attacks are common, targeting a medical institution is not.

“I have never heard of this kind of attack trying to shut down a hospital. This puts lives at risk, and it is sickening to see such an act,” he said. “Health management systems are beginning to tighten their security.”

The 434-bed short-term acute care hospital on Vermont Avenue is owned by CHC of South Korea.

Under federal law, hospitals are required to report potential medical data breaches involving more than 500 people.

Since 2010, at least 158 institutions, including medical providers, insurers and hospitals, have reported being hacked or having information technology issues that compromised patient records, federal records show.

Ransom attacks are still relatively rae. But cyberattacks on hospitals have become more common in recent years as hackers pursue personal information they can use for fraud schemes. Last July, hackers may have accessed as many 4.5 million patient records in UCLA Health System's computer network.

**For SoCal crime & investigations follow me on Twitter**[**@lacrimes**](http://twitter.com/lacrimes)

**ALSO**

[**Apple CEO says helping FBI hack into terrorist's iPhone would be 'too dangerous'**](http://www.latimes.com/local/california/la-me-apple-san-bernardino-terror-20160218-story.html#nt=oft12aH-1gp2)

[**The futile fight to save Autumn, a 1-year-old victim of gang violence in Compton**](http://www.latimes.com/local/crime/la-me-compton-baby-deputies-20160217-story.html#nt=oft12aH-1gp2)

[**Sentenced to prison for assault, teenage 'parachute kids' deliver warning to adults in China**](http://www.latimes.com/local/lanow/la-me-ln-parachute-kids-sentencing-20160217-story.html#nt=oft12aH-1gp2)