Codify
BY AAPC

Health Information Compliance Alert

Case Study: Should You Pay A Ransom To Get Your PHI Back?

Experts weigh in on what you should do in the event of a ransomware attack.

Jaws dropped in the healthcare industry as news broke of a hospital's decision to pay hackers a ransom to retrieve control of their computer systems. This case begs the question: Was the decision to give in and pay the ransom the right choice?

Background: On Feb. 17, **Hollywood Presbyterian Medical Center** announced that it paid 40 Bitcoins (equivalent to $17,000) to hackers that deployed malware into the hospital's computer systems, locking access and preventing the hospital from sharing electronic communications. Although the malware affected the hospital's electronic medical record (EMR) system containing patients' protected health information (PHI), the hospital claimed that patient care wasn't compromised, and that there is no evidence that any unauthorized access of patient or employee information occurred.

The malware locked Hollywood Presbyterian's systems by encrypting files, and then the hackers demanded that the hospital pay a 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," hospital President & CEO **Allen Stefanek** stated in the Feb. 17 memo.

Get Ready for Your Wake-Up Call

Reaction: "The Hollywood Presbyterian incident has been a huge wake-up call for healthcare and has finally allowed information security to have the respect it deserves in the boardroom," notes HIPAA expert **Jim Sheldon-Dean**, founder and direct of compliance services at **Lewis Creek Systems LLC** in Charlotte, VT. "Healthcare has traditionally been less sophisticated when it comes to information security ... [but] now is the time to get serious about protecting systems, because lives and institutions are at stake."

Problem: "Healthcare institutions are in a tough space," says **Larry Whiteside, Jr.**, Vice President of Healthcare and Infrastructure for **Optiv**, a Denver-based cybersecurity solutions firm. "They have low margins and have to figure out how to spend their money wisely. Security has for decades been their last choice of spend."

And despite cyber attackers' increases in sophistication, "unfortunately, hospital systems have not kept up with the times in changing their endpoint methodologies," Whiteside warns.

Could This Attack Be a Sign of a 'Pandemic?'

Like many industry experts, the attack on Hollywood Presbyterian didn't surprise Whiteside, but now there is more media attention on how healthcare organizations are easy targets for cyberattacks. "Healthcare data is more valuable to hackers than credit cards since more information can be gleaned from it," he notes. "It is the beginning of a pandemic hitting health systems in the next few years."

This isn't a "first-of-its-kind" attack, but it's the first to get a lot of publicity mostly because initially the media misreported the ransom as in the millions of dollars range, Sheldon-Dean notes. "These attacks have been underway for some time and are on the increase, to be sure."

Nevertheless, the Hollywood Presbyterian case has left many healthcare organizations feeling vulnerable and somewhat helpless. Fortunately, there are actions you can take to prevent and mitigate such an attack on your PHI.

Under Attack: Take 7 Steps

First: "Always defer to the recommendations of law enforcement and security experts when it comes to paying a ransom, so long as you consider what is best for the patients," Sheldon-Dean advises. "You need to do whatever is necessary to have essential information available, and that can certainly mean paying the ransom. Every situation is different, but it will come down to a decision about what is best for both the patients and the institution."

Here's what else experts advise that you do:

1. Back up your data regularly. Have good, regularly tested backups of your data that are separated from your networks and protected from alteration. "If your data gets locked up, you have something to work from and can perhaps avoid paying the ransom," Sheldon-Dean says. "If you don't, you don't really have a chance."

2. Have a contingency plan. "Be prepared to shut down your systems and networks and still provide care," Sheldon-Dean advises. Plan for how you will communicate and maintain records, and practice your paper-based methods regularly. Develop your plans and practice drills using these methods.

3. Arm yourself with good training and hygiene. "Education is low-hanging fruit once a year is not enough to train your people," Whiteside stresses. Healthcare organizations "must emphasize cybersecurity education" for their employees to ensure that they understand how best to mitigate risks.

4. Focus on endpoint devices. When it comes to ransomware viruses, "organizations have to work on security on their endpoint devices (smartphones or tablets)," Whiteside advises. These devices are more prone to cyberattacks now than ever before plus, the use of mobile devices is more prevalent and they have more access to data because they're interconnected.

5. Enlist information security experts. "If you're attacked, get the best information security experts you can afford to see if there is a way out and to keep from damaging any evidence you may need to preserve," Sheldon-Dean recommends.

6. Contact law enforcement. "If there has been an intrusion, you should call your state police's cybersecurity task force, or its equivalent, to get law enforcement involved," Sheldon-Dean says. "Don't be rash, and don't publicly state there is a threat or not until you actually know."

7. Make your decision carefully. Whether to pay a ransom is a "business-based risk decision," according to Whiteside. If patients' lives are not at risk, you might choose not to pay the ransom and even if you do pay the ransom, "there is no guarantee that you will get access to your data back."