COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 21, Number 7. July 08, 2021 Rash of Ransomware Attacks Shows Inevitability, Imperative to Prepare

By Jane Anderson

Ransomware experts agree: Bad actors are targeting the health care sector at an accelerated pace, and if an organization lacks safeguards, it is at high risk of a data breach.

Cybercriminals view every type of organization as a moneymaking opportunity, said Rebecca Herold, president of SIMBUS360 and CEO of The Privacy Professor. However, small and mid-sized organizations can be particularly fruitful targets for them because those smaller organizations—which include many covered entities (CEs) and business associates (BAs)—don't have dedicated positions for cybersecurity.

"Every CE and BA will be targeted at least once, but often many times," Herold told *RPP*. "CEs and BAs will get hit with ransomware from at least one of the attempts if they do not provide sufficient training and keep awareness high within their workforce. They will then end up paying if they do not have a sufficient backup and recovery plan in place." Herold added that "all these ransomware attacks have revealed that far too many organizations are woefully lacking in such preparedness."

Ransomware spiked during the COVID-19 pandemic, and has reached seemingly epidemic proportions within the health care industry. A sampling of recent incidents reveals a wide range of organizations affected, with varying impacts:

- **St. Joseph's/Candler, the largest hospital system in Savannah, Georgia, first detected a ransomware attack on June 17 that hobbled some systems**. Restoration efforts continued into the end of June, according to a statement from the hospital system on June 29: "St. Joseph's/Candler continues to make progress on our restoration efforts and has activated certain clinical systems. We have been and continue to admit and care for patients. We will continue to work methodically to restore remaining systems as quickly and safely as possible."[1]
- **Ransomware at a fertility treatment provider in Atlanta resulted in a data breach that exposed sensitive personal and medical information of around 38,000 patients, according to the organization**. Reproductive Biology Associates (RBA), which also co-founded MyEggBank, the largest network of donor egg banks in North America, said in its notice that the clinic first became aware of an incident on April 16.[2]

  The organization discovered that "a file server containing embryology data was encrypted and therefore inaccessible." According to the organization, "we quickly determined that this was the result of a ransomware attack and shut down the affected server, thus terminating the actor's access, within the same business day." RBA said the hacker "first gained access to our system on April 7, 2021 and subsequently to a server containing protected health information on April 10, 2021."

  During the investigation, RBA said, "access to the encrypted files was regained, and we obtained confirmation from the actor that all exposed data was deleted and is no longer in its possession." The fertility organization also said that "in an abundance of caution, we conducted supplemental web searches for the potential presence of the exposed information, and at this time are not aware of any resultant exposure." Full names, addresses, Social Security numbers, laboratory results and "information relating to the handling of human tissue" was exposed in the breach, the organization said.

- **An attack that a consultant said could be ransomware hit University Medical Center in Las Vegas in late June.**[3] The hacker group REvil began posting personal information online purportedly obtained in the cyberattack, including images of Nevada driver's licenses, passports and Social Security cards for around half a dozen alleged victims. Hackers sometimes post data online in an effort to push an entity to pay a ransom demand.

  After receiving an inquiry from the *Las Vegas Review-Journal*, University Medical Center issued a statement confirming that cybercriminals in mid-June accessed a server used to store data. "This type of attack has become increasingly common in the health care industry, with hospitals across the world experiencing similar situations," the medical center said.