Privacy & Security Law Report®

March 26, 2018

Bloomberg BNA

Privacy

# Speedy Action Is Key to Resolving Health-Care Hacks

**BNA Snapshot**

- Hospitals and providers need to respond fast to data breaches
- Waiting too long can harm reputation, lead to financial damages


By James Swann

A recent New York hospital data breach has highlighted the need to inform patients as soon as possible or face potential financial consequences.

Albany, N.Y.-based St. Peter's Surgery & Endoscopy Center discovered hackers had breached the hospital's computer network Jan. 8 but waited until Feb. 28 to notify patients and the government that private health records might have been compromised. The breach may have compromised roughly 135,000 patient records, including patient names, diagnosis and procedure codes, and insurance information.

A data breach is a nightmare for any health-care organization and an increasingly likely one as hackers grow more sophisticated, making it essential to prepare a reaction plan ahead of time to minimize the financial costs.

For example, the government announced a $3.5 million settlement with Fresenius Medical Care North America in February over the handling of five separate data breaches at Fresenius facilities across the country. Fresenius provides services to patients suffering from chronic kidney failure.

It can take a long time to run a full forensics investigation after a data breach to determine whether any patient records were accessed, and starting right away is essential, Adam Greene, a privacy attorney at Davis Wright Tremaine in Washington, told Bloomberg Law.

“Because HIPAA doesn't allow an unreasonable delay of breach notification, covered entities and business associates should document what they did and when they responded to an incident so that they can demonstrate that the breach notification wasn't unreasonably delayed,” Greene said.

The Health Insurance Portability and Accountability Act requires health-care providers and their contractors to safeguard the privacy and security of patient medical records. It also requires organizations to notify affected patients and the government within 60 days of discovering a data breach.

Data breach investigations are complex and require time due to their fact-sensitive nature, Melissa Markey, a health-care attorney with Hall, Render, Killian, Heath & Lyman PC in Detroit, told Bloomberg Law.

“Having a written incident response plan with all the key internal and external players identified is helpful when responding to security breaches quickly and effectively,” Markey said.

The Health and Human Services Office for Civil Rights is investigating the St. Peter's Surgery incident, which is the second largest breach of 2018, following a 280,000 record breach at the Oklahoma State University Center for Health Sciences that was reported to the OCR Jan. 5.

St. Peter's didn't respond to a request for comment on the breach.

## Best Practices

The 60-day deadline for notifying patients and the government is a bright line, and there's not much wiggle room in terms of late notifications, Iliana Peters, a health-care attorney with Polsinelli PC in Washington, told Bloomberg Law.

Health-care organizations need to meet the deadline with whatever data they've collected on the breach, Peters said. The looming deadline makes it essential for health-care organizations to have pre-existing breach-response plans in place, Peters said.

Hospitals and physicians practices may not think about these issues when they contract with business associates, and find themselves scrambling to conduct an investigation once a breach happens, Peters said.

A four-step plan can help companies handle a breach, Peters said, with the first step dedicated to “stopping the bleeding.” “You're leaking data, and you need to figure out where the hole is and stop it,” Peters said.

A second step is to cooperate with law enforcement. In certain cases law enforcement can ask for breach notifications to be held due to ongoing investigation, and in that case the 60-day deadline doesn't apply, Peters said.

As a third step, companies should work with information-sharing organizations, which collect information on data breaches and disseminate it to the rest of the industry. The last stage involves fulfilling the legal obligation to notify patients and the government, Peters said.

Breach investigations take time, and you don't want to jump the gun too soon on notifying patients and the government and end up having to amend your original notification, Peters said. It's better to have good data that you can share with patients and the government rather than being forced to backtrack repeatedly, Peters said.

“Unfortunately, health-care breaches will happen more often, because the data is where the value is,” Peters said.

## Cyber Risks

The St. Peter's breach is another confirmation that health-care providers are facing growing cybersecurity risks based on the large amount of sensitive personal data they maintain, Laura Hammargren, a health-care attorney with Mayer Brown LLP in Chicago, told Bloomberg Law.

Investigating a cyber attack can be a complex process, which explains why there's often a lag between when the breach was discovered and when notifications were sent to patients, Hammargren said.

A hacked health-care organization needs to determine how the hack happened, how many patient records were impacted, and what kind of information was in the records, Hammargren said. Health-care organizations can speed up this process by laying the groundwork before an attack occurs, including conducting a detailed security risk analysis and preparing a contingency plan, Hammargren said.

Cyberattack simulations can also help a health-care organization practice what to do in case of a real attack, Hammargren said.

To contact the reporter on this story: James Swann in Washington at jswann1@bloomberglaw.com

To contact the editor responsible for this story: Kendra Casey Plank at kcasey@bloomberglaw.com