AHLA WEEKLY
3/10/2017

Think Outside the Breach: Six Legal Issues to Consider After Responding to a Cybersecurity Incident

By Kristin J. Jones and Jana M. Landon, Stradley Ronon Stevens & Young LLP

Alert! Your files have been encrypted. To obtain a decryption key, you are required to pay 500 USD within the next 72 hours. Failure to do so—or any attempt to remove or damage this software—will result in the immediate destruction of all files.

The health care industry is sophisticated when it comes to data privacy and cybersecurity, but security incidents still happen. When an organization discovers a security incident—whether a ransomware alert like the one above, a stolen laptop or USB drive, or a compromised system password—the incident response processes should, ideally, immediately spring into motion. During a ransomware attack, for example, the information technology team may shut down the affected units (or servers) and may have to shift operations to back-up servers in accordance with a business continuity plan. Law enforcement is often notified, and police reports are routinely filed. The team keeps detailed written records of the steps they take to resolve the incident. Everyone breathes a sigh of relief that the crisis is over and gets back to their regular work.

But the work is not done. The health care industry—particularly attorneys, privacy officers, and risk managers—must "think outside the breach" and consider the secondary effects of a security incident. The steps a health care organization takes after the incident is resolved from a technical perspective can significantly impact the organization's financial exposure, litigation risk, and reputation. Among these defensive measures are:

1. Notifying patients, the Office for Civil Rights, and other agencies

Both federal and state laws establish requirements for breach notification. Laws can be inconsistent and require notification to different people on different timetables. Even the definition of what constitutes a "breach" varies significantly under these laws.

Most obviously, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires notification following the discovery of a breach of unsecured protected health information.[1] Following a breach, HIPAA gives covered entities 60 days to notify individuals affected by the breach, the Office for Civil Rights (OCR) of the Department of Health and Human Services (HHS), and even the media in certain circumstances. To determine whether a breach has occurred under HIPAA, covered entities must conduct an incident risk assessment, which is an analysis that evaluates the risk that patient data was compromised. An incident risk assessment uses a four-factor approach. It considers (1) the nature and extent of the compromised information; (2) the party who accessed the information; (3) whether the information was actually viewed or acquired; and (4) the extent to which the risk of compromise was mitigated.

Many covered entities are shielded from this reporting obligation because they encrypt electronic data that is covered by HIPAA. The HHS Secretary has declared that encrypted electronic protected health information is deemed secure; accordingly, the loss of encrypted data generally does not qualify as a breach under HIPAA. Health lawyers evaluating whether a security incident constitutes a reportable breach should use caution in relying heavily on encryption because HHS has also

determined that covered entities may still have a reportable breach when encrypted data is further encrypted by ransomware software.

Even health lawyers who are well-versed in HIPAA breach notification may neglect to check applicable state breach notification laws. State breach notification requirements can vary widely and are constantly changing. Florida and Illinois are two states that demonstrate the differences in state law. In Florida, entities have 30 days to notify individuals of a breach affecting more than 500 Florida residents, or will face a fine up to $500,000.[2] By contrast, Illinois wholly exempts HIPAA-covered entities from its state notification requirements, as long as the covered entity provides notice to the Illinois Attorney General within five days of notifying the Secretary.[3] Breach counsel should carefully review the state breach notification laws in every state where affected individuals reside to determine which state laws are implicated. Further, what constitutes a breach can vary widely. All states with data breach laws, for example, follow HIPAA's lead and have determined that if encrypted information was accessed and there is no indication that the encryption was compromised, no notification is required. The District of Columbia, however, has no such encryption "safe harbor."

2. Preparing for the inevitable HIPAA audit

If an organization's breach notification obligations included reporting a breach to OCR, the organization should anticipate an OCR investigation shortly thereafter. Covered entities and business associates alike are at risk for an OCR audit following a breach.

As soon as practicable after mitigating the breach, organizations should initiate a review of their HIPAA policies and procedures to make sure that all required policies are in place, current and, most importantly, followed by the workforce. Even if the organization recently completed comprehensive HIPAA training, it should consider a targeted training focused on the security incident or breach. If third-party vendors were implicated in the breach, the organization should review business associate agreements, conduct security audits, and possibly initiate action against the vendor responsible for the breach.

In preparing for an audit, organizations should pay particular attention to the policies and other documentation related to the breach or other recent security incidents. OCR will ask why the breach occurred and how the organization will prevent similar breaches in the future. Breach counsel should anticipate OCR's inquiries and ensure that the organization can demonstrate strong privacy and security initiatives, consistent with HIPAA's requirements.

3. Revising the organization's policies and procedures

As discussed above, a post-breach OCR investigation necessitates a close review of the organization's HIPAA policies and procedures. Even in the absence of a HIPAA audit, the organization should revisit its privacy and security policies to incorporate any lessons learned during the incident. The organization should consider, among other things, whether any deficits in current policies lead to the security incident or if the workforce was not adequately trained on the existing policies.

In addition to policies addressing the organization's handling of data, the incident response plan is a ripe area for review after a security incident. Incident response plans provide instructions and steps for the organization to take when responding to a security incident. An incident response plan helps the organization react to a cybersecurity incident in an organized way. Having an established incident response plan—and an incident response team familiar with its responsibilities in the wake of an incident—can ensure a swift and effective resolution to a security incident.

After a security incident, organizations should review the incident response plan to evaluate whether it followed its incident response plan when it responded to the actual security incident. If the organization may discover that some aspects of the incident response plan were too burdensome or inefficient to implement practically, it should revise the plan to reflect better practices. Alternatively,

the team may not have followed the policy due to training deficiencies. If so, the organization should consider additional training for the incident response team, ideally including realistic desktop exercises.

4. Complying with the organization's cybersecurity insurance policy

Organizations cannot prevent—or fully remediate—every cybersecurity incident. Cyber insurance can help cover the costs of forensic investigations, legal advice, business interruption losses, breach notification expenses, credit monitoring costs, reputational harm, cyber extortion, and data loss or destruction. It is, therefore, an important part of any health care organization's risk management toolkit. Policies can also protect against liability for claims brought by customers and employees suffering a breach of privacy due to a cyber event, claims for statutory privacy violations, and costs for responding to regulatory inquiries relating to a cyber event, including costs associated with investigations, fines, and penalties.

Even for organizations that have cyber insurance policies, coverage may be insufficient and insurers may limit coverage if the organization does not use a specific outside lawyer or forensic expert. Before engaging the organization's preferred vendors, counsel should review the policy to identify any prerequisites for full coverage. Organizations reading this article before experiencing a cybersecurity incident should consider contacting their insurance broker to ask about adding preferred vendors and attorneys to the organization's cyber policy.

5. Mitigating class action lawsuits

Although HIPAA does not give consumers a right to sue covered entities or business associates, data breaches may nonetheless lead to class action lawsuits. The theory underlying these cases is that the organization could have avoided the breach by taking reasonable steps to protect its system from cyber attacks; this is generally alleged in the form of a negligence claim.

In the retail space, consumer-driven claims are usually subject to motions to dismiss on the basis of standing; organizations argue that consumers cannot prove any cognizable harm as a result of a data breach. When the data breach exposes patient health data, organizations have a more difficult time defending against patients' claims. For example, the class action lawsuit filed following the famed Anthem breach, for example, survived several motions to dismiss.[4] Additionally, St. Joseph Health System in California recently settled a consumer class action for $15 million after spending $17 million on security improvements and $4.5 million on credit monitoring services to breach victims.[5] Shareholders and financial institutions may initiate class action lawsuits for costs, such as expenses arising from reissuing credit cards or covering fraudulent charges, after a patient's financial information was used inappropriately.

Although class action lawsuits are unavoidable, organizations can take steps to protect themselves against liability. Because the lawsuits are generally based in negligence, the organization can defend itself by showing that it acted reasonably in preparing for and responding to the breach. Accordingly, following an incident, the organization should retain counsel early to direct it through the data breach process, with an eye toward potential litigation. It should clearly document how it identified the problem, what steps it took to mitigate or resolve the incident, and efforts it took to notify individuals about the breach. The organization should work toward building a strong case that it responded reasonably to the incident in anticipation of defending potential lawsuits. Additionally, the organization, with the support of its attorneys, should consider engaging a public relations firm to manage the message and limit reputational damage caused by a class action.

6. Preparing for the next cybersecurity incident before it happens

All organizations should anticipate security incidents before they occur. The organization's first security incident is a wake-up call—a reminder that the organization must strengthen its security policies, review HIPAA policies, and train employees. Organizations should regularly evaluate their HIPAA policies, conduct tabletop exercises with their incident response plan, encrypt data, perform

risk assessments, audit third-party vendors, and more in order to catch security vulnerabilities before they happen.

An ounce of prevention is worth a pound of cure. Likewise, preventing a security incident before it happens is the best way to resolve a security incident. Organizations, particularly those in the health industry, cannot prevent all incidents. When the organization responds to an inevitable security incident, remember to think outside the breach!

Kristin J. Jones provides regulatory, compliance and reimbursement counsel to health care providers (including hospitals, health systems and physician practices) and insurers. Kristin counsels clients who operate in a highly regulated environment and is skilled at providing practical advice about complex regulatory schemes.

Jana M. Landon co-chairs Stradley's Data Breach Response and Cyber Insurance teams. She is also founder and chair of the firm's E-Discovery Team. Her practice focuses on advising organizations of all sizes in multiple industry sectors on data breach response, data security and data management issues. Jana also provides regulatory compliance services and assists clients in policy/procedure preparation, tailored by the client's specific risks and governing laws.

[1] 45 C.F.R. § 164.404(a)(1).

[2] Fla. Stat. § 501.171(4) (2014).

[3] 815 Ill. Comp. Stat. 530/50 (2017).

[4] *See In re Anthem Blue Cross Affordable Care Act Cases*, Case No. JCCP4805 (Cal. Super. Ct., County of Los Angeles).

[5] *See HIPAA Journal*, St. Joseph Health Settles Class Action Data Breach Lawsuit, http://www.hipaajournal.com/st-joseph-health-settles-class-action-data-breach-lawsuit-3354/.