HCCA
hcca-info.org

Compliance TODAY

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

APRIL 2018

A smooth transition

an interview with
Gerry Zack
Incoming CEO
SCCE & HCCA

ARTICLES

Compliance TODAY

Compliance Today (CT) (ISSN 1523-8466) is published by the Health Care Compliance Association (HCCA), 6500 Barrie Road, Suite 250, Minneapolis, MN 55435. Subscription rate is $295 a year for nonmembers. Periodicals postage-paid at Minneapolis, MN 55435. Postmaster: Send address changes to Compliance Today, 6500 Barrie Road, Suite 250, Minneapolis, MN 55435.

VOLUME 20, ISSUE 4

by Bethany A. Corbin, JD

Data breach compliance after Uber: Avoiding scandal

» Data breaches are inevitable, but compliance responses can mitigate damage.
» Breach notification alone should not drive the investigation process.
» Inventory your sensitive data to identify system vulnerabilities.
» Incident response plans can lead to effective breach response strategies.
» Breach validation and containment are crucial to mitigation.

Bethany A. Corbin *(bcorbin@wileyrein.com) is an attorney at Wiley Rein, LLP in Washington, DC and focuses her practice on healthcare, privacy, and cybersecurity.*

Like the latest installment of the *Star Wars* saga, data breaches are highly anticipated, command strong media attention, and can impact the lives of millions of consumers. From Anthem Blue Cross to Banner Health to Equifax, security-related incidents have dominated headlines and remain a top concern for businesses in 2018. In a survey of more than 15,000 chief information security officers (CISOs), the Ponemon Institute found that 67% of CISOs believed their companies would likely experience a cyberattack or data breach this year, with 60% noting that their concern has increased since 2017.[1,2]

Healthcare entities in particular are prime targets for data breaches, given the sensitive information contained in medical records. From January to June 2017, hackers accessed almost 1.6 million patient records, and insider wrongdoing further exposed another 1.17 million patient records.[3] Failure to appropriately secure data and implement timely responses and notification measures for breaches can expose healthcare organizations to reputational damage, investigative inquiries, and civil liability. Given the organizational risks associated with data breaches, it is unsurprising that the term conjures images of fear for both companies and consumers, much like the *Star Wars* Death Star inspired dread throughout space civilizations.


Corbin

The inevitability of data breaches has forced companies to question their prevention and response strategies—particularly in light of Uber's recent data breach scandal. Although the popular press has taken issue with Uber's failure to follow data breach notification laws, adherence to such laws alone will not ensure a culture of compliance—especially in the healthcare industry. Rather, an effective compliance response to healthcare data breaches must begin before a breach occurs and continue after the breach is contained. Breach notification is an important aspect of compliance, but contrary to widely held belief, it should not dominate the compliance and investigative process. Instead, organizations

must focus on identifying, containing, and remedying the breach as top priorities. This article proposes three compliance strategies for healthcare entities to employ before, during, and after a data breach to help avoid becoming the next Uber.

Before a data breach

Knowing what kinds of protected information your organization handles, where it is stored, and who handles it and why (both in-house and with vendors) is key to keeping that data safe. An incident response plan will help you respond effectively to a possible threat.

Inventory and monitor protected health information

If your organization collects, maintains, or uses protected health information (PHI) (as that term is defined by the Health Insurance Portability and Accountability Act [HIPAA] and relevant state law), you should review and analyze your information systems to identify where your company stores PHI and other sensitive data.[4] An inventory of protected information can help confirm your compliance with state and federal laws. This inventory should provide a complete summary of every element of PHI that your organization possesses—in both paper or electronic format. An easy way to begin the inventory is to follow the path of PHI through your organization from the time a patient contacts your organization until the final claim is paid, accounting for each person and system that handles PHI. Consider documenting the types of PHI and sensitive information that your organization maintains and how this data is kept secure. By understanding the flow of sensitive data, your organization can respond faster to a breach and will have an immediate sense of whether the system hack involved sensitive information. Following this inventory, you should continue to review and update your information systems, and monitor for PHI and data leakage or loss.

Develop an incident response plan and risk mitigation strategy

An incident response plan (IRP) is a key organizational document that converts knowledge into a step-by-step actionable framework for use during a data breach. In essence, the IRP should be a written data breach response policy that identifies the appropriate individuals to contact during a breach, sets forth required documentation efforts, and highlights response strategies. Legal standards, including breach notification requirements, should also be incorporated into this document.

Consider identifying the appropriate incident response team in the IRP, which may include the chief privacy officer, general counsel, administrators, IT professionals, and risk management representatives. The individuals on the team should be empowered to react to a data breach, and should receive applicable training on data breach response and mitigation. Further, your IRP should specify incident handling procedures and should ensure that all employees know how to timely report data breaches. Ensuring effective internal communication is key during a data breach, and each employee should be reminded of the time sensitivities associated with compromised PHI. When they occur, data breaches are stressful events, and the creation of a well-executed IRP can minimize the impact and uncertainty associated with a breach.

Assess and understand vendor vulnerabilities

In the age of outsourcing, most healthcare organizations rely heavily on approved vendors to conduct certain business operations. As the Health Information Technology for Economic and Clinical Health (HITECH) Act

made clear, business associates that work for covered entities and have access to PHI must comply with HIPAA. The HITECH Act expanded liability for both business associates and covered entities in the event of a breach, and covered entities may be liable for breaches that occur within the vendor organization.

Accordingly, it is crucial that covered entities understand their legal and compliance obligations with respect to vendors. Indeed, the Equifax hack recently exposed theoretical healthcare vendor vulnerabilities.[5] Equifax operates as a financial verification vendor to the Department of Health and Human Services for enrollees under the Affordable Care Act. Equifax's marketplace exchange data was not implicated in the breach, but it serves as a cautionary tale of how vendors can leave covered entities vulnerable to attack. Healthcare data breaches premised on vendor vulnerabilities are increasingly common, and data sharing with third parties is perceived as one of the biggest vulnerabilities for healthcare providers. Thus, covered entities should attempt (to the best of their ability) to actively monitor their vendor's privacy and security compliance, and ensure that effective and clear lines of communication exist for vendors to report data breaches to the covered entity.

If it's too late to prevent a breach, you should focus on taking steps to minimize the impact and limit further damage.

During a data breach

If it's too late to prevent a breach, you should focus on taking steps to minimize the impact and limit further damage.

Validate and contain the breach

When faced with a data breach, your organization should respond immediately to verify and contain the breach.[6] The goal here is to stop the bleeding as swiftly as practical. Identify the affected systems and work to segregate affected servers or endpoints. Determine the type of information disclosed and its sensitivity level, which will help guide your mitigation plan and subsequent notification requirements, if any. Not every breach will involve PHI, and it's important to recognize the level of confidentiality associated with the breached data. Further, you should evaluate whether the breach is ongoing (e.g., system hack) or sufficiently limited in scope (e.g., lost flash drive or laptop). If the breach is continuing, take immediate action to prevent further data loss.

Consider isolating and containing any infected system to prevent additional damage until a long-term solution can be devised. If the breach involved a loss of property, such as a laptop containing PHI, investigate whether the device can be recovered. If recovery is successful and it is evident that the sensitive data had not been accessed, breach notification may be unnecessary.

Implement your incident response plan

After taking steps to contain the immediate breach threat, your organization should implement its IRP. The IRP will specify notification procedures for the incident response team, and these individuals must be apprised of the status of the breach and any efforts taken to contain or stop the breach. Effective internal communication during and after a breach is essential to mitigate damage, and the incident response team will likely need to coordinate communication among multiple organizational units. Additionally, be sure to

document all mitigation efforts and response measures, as this will be crucial for evaluating the effectiveness of your IRP and can serve as favorable evidence in a subsequent investigation.[7]

Notify legal counsel and insurers

With the breach contained and your IRP implemented, you should determine if notifying legal counsel and relevant insurance companies is warranted.[8] Involving an attorney at an early stage in the breach investigation will permit maximum use of the attorney-client privilege. This doctrine limits access to certain privileged communications between attorneys and their clients, and it can prevent those communications from being disclosed during subsequent investigations or lawsuits.

The lawyer you contact should be familiar with your company's business structure, operations, policies, and risk management plan, and should also possess substantive knowledge of data breach laws. In addition to notifying your attorney, you should also alert any relevant insurance companies that a breach occurred. Insurers have extensive experience dealing with data breach mitigation and may offer helpful strategies and suggestions. Data breaches often grow in scope and size from what is originally anticipated, so involve your insurer early—even if you don't think the damage from the breach will exceed your policy's limits.

After a data breach

After the fire is out, you may need to notify the appropriate federal, state, and local authorities, as well as the consumers affected by the breach. A post-mortem of your response plan will also help you make improvements and demonstrate that your organization is serious about handling breaches.

Investigate and fix vulnerable systems

Following the immediate aftermath of a data breach, it is necessary to investigate the cause of the breach and mitigate harm. Learn as much as possible about the root cause of the breach. For example, if a laptop containing PHI was stolen, determine how an unauthorized individual obtained access to the laptop. Were there insufficient physical controls, such as locks, that enabled access? This investigation may require the involvement of technical specialists and professionals, including forensic investigators.

Even if a data breach is limited in scope and contained, it is essential to determine why the breach occurred and remedy the underlying vulnerability. Liability for data breaches is often more severe if an organization had knowledge of a vulnerability but failed to fix it, and insurance companies may refuse to cover breach incidents where the company purposefully failed to act in light of this information. Data breaches should thus be viewed as an opportunity to remedy vulnerabilities and enhance organizational security.

Comply with breach notification laws

Once your organization has investigated the cause of the breach and determined whether PHI was exposed, it's time to address compliance with breach notification laws. The HIPAA Breach Notification Rule is a comprehensive regulation that outlines organizational procedures for the unauthorized use or disclosure of PHI, and the majority of states have enacted their own breach notification statutes. Accordingly, healthcare entities may be subject to two or more breach notification standards, depending on the relevant jurisdiction(s). HIPAA does not preempt more stringent state laws, and numerous state statutory frameworks specify the required contents of a breach notification. Notification under HIPAA may take a slightly different form

than notification under state law. The legal counsel you consulted during the breach can assist with navigating the technicalities of these laws.

Although healthcare organizations must comply with both federal and state laws, not all breaches require notification. For instance, although PHI may have been contained on a stolen laptop, HIPAA and most state statutes do not require notification if the PHI was encrypted and the encryption key was not similarly accessed.[9] Additionally, some breach notification statutes incorporate a risk of harm analysis, and if the risk of harm to consumers is sufficiently low, notification is not required. Be sure to check local regulations for documenting this risk of harm analysis, and ensure that consultation with a relevant state agency is not required. It's important to review the federal and state laws directly applicable to your organization to determine if breach notification is even a relevant concern. If notification is required, consider involving your Marketing or Public Relations department to help craft notification statements and press releases.

Review and revise the incident response plan

Finally, it's important to analyze the effectiveness of your IRP after it has had a chance to work in action. Did your IRP work smoothly? Were there glitches in communication that need to be resolved? What improvements can be made? Every data breach incident is a learning experience, and you should take time to consider the strengths and weaknesses of your IRP. The early documentation that you kept in implementing the IRP can be particularly helpful in determining where improvements can be made. Understanding and fixing weaknesses is essential to enhancing organizational security and goes a long way towards demonstrating a strong commitment to compliance.

Conclusion

The threats associated with data breaches are daunting. As the healthcare industry becomes increasingly connected, these threats will multiply in number and magnitude over the coming years. We can't use the "force" to stop data breaches and hackers, but organizations can strengthen their internal security controls, response plans, and compliance frameworks to handle breaches in a comprehensive and effective manner. By implementing effective compliance controls, organizations can guard against scandal and improve the security of patient data.

1. Opus: "What CISOs Worry About in 2018: A Ponemon Institute Survey, January 9, 2018." Available at http://src.bna.com/vAu
2. Jimmy H. Koo: "Data Breaches Remain Top Concern for Chief Information Security Officers in 2018" *BNA Privacy & Data Security Blog*; January 11, 2018. Available at http://bit.ly/2Dync1N
3. Protenus, Inc.: "2017 Breach Barometer Report: Mid-Year Review" Available at http://bit.ly/2nEbP1y
4. See Privacy Technical Assistance Center: Data Breach Response Checklist. Available at http://bit.ly/1hon1tn
5. Dave Barkholz: "Equifax Breach Exposes Healthcare Vendor Vulnerabilities" *Modern Healthcare*; September 12, 2017. Available at http://bit.ly/2r6Ghpf.
6. Kirk Nahra and Edward Brown: "Responding to Security Breaches" *The Practical Lawyer*; October 2016. Available at http://bit.ly/2DhTq3r.
7. Robert Lord: "You've Had a Health Data Breach – Now What?" *Compliance & Ethics Blog*; February 14, 2017. Available at http://bit.ly/2EJQNVs.
8. Ibid, Ref #6, at 41.
9. 45 C.F.R. § 164.402 (Modified definition of a breach, effective March 26, 2013)