COSMOS
Navigate the Compliance Universe

Compliance Today - April 2018
Data breach compliance after Uber: Avoiding scandal

By Bethany A. Corbin, JD

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.

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.