Avoid Pain After a Breach—Read the Fine Print

Save to myBoK

By Joe Gillespie, MS, RHIA, CHPS, and Susan Lucci, RHIA, CHPS, CHDS, AHDI-F

The Anthem Blue Cross breach made the cybersecurity data breach headlines across the nation in 2015. As the single largest email phishing attack up until that time, impacting nearly 80 million patients, this breach essentially changed the privacy and security world as we knew it. No longer was cybercrime something that happened only in retail stores involving credit cards. The bad guys had figured out where to find massive amounts of valuable data—and they knew exactly how to get it.

While credit cards are a common target, when a credit card is compromised the owner of the card typically can contact the bank, take care of the charges, and get a new card relatively quickly. The individual impact is generally short-lived and the inconvenience is pretty easily remedied, in the majority of cases, within a few days. A breach of protected health information (PHI), which most often includes personally identifiable information (PII), is far more intrusive and can last as long as the criminals choose to "keep" the information.

In the Anthem case, through a long and exhaustive investigation, it was determined the breach started with a single click by an employee who thought they were opening a legitimate email. Initial unauthorized access started on December 2, 2014, and continued until the date of discovery on January 27, 2015.

Once the investigation and reporting process was started, it took the US Department of Health and Human Services' (HHS)Office for Civil Rights (OCR) until 2018 to conclude their investigation and enter into a settlement agreement with Anthem. OCR alleged the following HIPAA Security Rule violations:[1]

- Failure to conduct security risk analysis—45 C.F.R. § 164.308(u)(1)(ii)(A)
- Failure to review records of information system activity—45 C.F.R. § 164.308(a)(1)(ii)(D)
- Failure to detect security incident which leads to a breach—45 C.F.R. § 164.308 (a)(6)(ii)
- Failure to implement technical policies and procedures pertaining to systems that maintain ePHI, allowing only authorized individuals to access that ePHI—45 C.F.R. § 164.312(a)
- Failure to prevent unauthorized access of ePHI maintained in a data warehouse—45 C.F.R. § 164.502(a)

Beyond the OCR Fine

As with most large breaches, the settlement agreement included a corrective action plan (CAP) with Anthem. The settlement amount was a whopping $16 million, the largest ever, and the CAP will likely take approximately two years or longer to complete. As severe as this may be, this was not the end of the financial pain for Anthem.

The costs to Anthem go far beyond the $16 million OCR settlement agreement. Anthem paid $2.5 million to retain expert consultants to investigate the breach, $115 million to improve security within the organization as the result of a class action lawsuit,[2] $31 million to provide individual notification along with notification to the general public, and an additional $112 million for 24 months of credit monitoring for the 19.1 million individuals who were able to demonstrate that their personal information was stored in the data center that was hacked.

Reading the Fine Print

The irony in looking back at this massive breach is that Anthem took the time to invest in HITRUST Certification in 2013.[3] Certainly, to their credit, the organization wanted to demonstrate their commitment to protecting their members' data. But when it comes to assurances and insurance in general, one must *read the fine print*. An article titled "Did Anthem's Security Certification Have Value?" by Marianne McGee, published on BankInfoSecurity.com, questioned the HITRUST common security framework (CSF) certification process. HITRUST responded that their certification process is based on a defined scope and the system breached was not in scope of their CSF certification.

Similarly, purchasing cyber liability insurance without properly complying with all aspects of the requirements or scope of that particular policy will not cover all that's needed in the case of a security incident. If the organization has failed to complete detailed tasks specifically called out in the fine print in order to validate the policy, claims against the policy may not be paid. Stated another way, if the cyber policy says that an organization must train employees in HIPAA privacy and security awareness, and that's not done, the insurance company is likely to not pay the claim. Or, if they do pay, and later determine that the organization was not adhering to its own policies and requirements of the HIPAA Privacy Rule and HIPAA Security Rule, they could demand a refund for claim dollars paid.

An instance of a claim that was paid and later a counter-claim asked through legal action for reimbursement happened in California where the healthcare organization had the insurance but no coverage. The important factor in this case comes as no surprise—at the end of the day, risk analyses and risk mitigation plans are an organization's most important security documents.[4]

The HIPAA Security Rule requires a risk analysis be completed on all systems and assets where PHI potentially resides. This is never a one-and-done process. Risk analyses must be performed annually and for all owned facilities. It is essential that biomedical devices are not overlooked. Recently, HHS has published guidance surrounding the vulnerabilities that may exist with these critical care systems.[5]

The Anthem breach was insider-oriented—one employee, one email. Insurance and certifications cannot protect healthcare organizations from all breach events. One of the best protections and investments an organization can make is in ongoing quality cybersecurity education for its workforce. It is equally important to ensure that business associates are keeping up with the changes in cybersecurity awareness. Specific education surrounding the pervasiveness of phishing attacks should be a high-priority item on every privacy officer's to-do list.

On the security side of the house, security professionals should find out when the last comprehensive security risk analysis was completed and updated. This is a task that should be completed and updated annually, without exception. The failure to do this was the foundational basis for the denial in the cyber liability denial claim mentioned above.

Keep the Workforce Vigilant

A thorough, well-planned training program for the workforce includes information on phishing attacks, what they look like, how to report them, and how seriously they can affect an organization. This is an imperative for 2019. Conducting an active phishing campaign can help keep the workforce vigilant and avoid the problems experienced by Anthem and so many other organizations.

There is no certification for HIPAA compliance and even with the best policies, training, and vigilance, security incidents can and will continue to happen. What health information management professionals can do is keep the workforce well-informed on the pervasiveness and creative nature of cybercriminal activity as it may be the best defense in this ongoing battle. Next, conduct a robust risk analysis process and update it methodically every single year. Risk profiles change every year as new equipment and systems are purchased and as new settings and upgrades are incorporated into existing systems. Finally, keep policies updated and review incidents with the privacy and security committee to ensure that a proactive stance is being taken to prevent new incidents from occurring in the same way they did before. Start now to minimize the risks of a privacy or security breach in 2019.

Notes

1. "$16 Million Anthem HIPAA Breach Settlement Takes OCR HIPAA Penalties Past $100 Million Mark." HIPAA Journal. October 16, 2018. www.hipaajournal.com/16-million-anthem-hipaa-breach-settlement-takes-ocr-hipaa-penalties-past-100-million-mark/.
2. "Court Approves Anthem $115 Million Data Breach Settlement." HIPAA Journal. August 20, 2018. www.hipaajournal.com/court-approves-anthem-115-million-data-breach-settlement/.
3. Anthem. "Health Information Trust Alliance Designates WellPoint Common Security Framework Certified Status." Press release. September 30, 2013. https://ir.antheminc.com/news-releases/news-release-details/health-information-trust-alliance-designates-wellpoint-common?ID=1859782&c=130104&p=irol-newsArticle.

4. Mitby, John. C. "Cyber Liability Insurance: Consider—But Be Careful as Insurance Company May Deny A Claim." Hurley Burish S.C. Attorneys blog. https://hurleyburish.com/cyber-liability-insurance-consider-but-be-careful-as-insurance-company-may-deny-a-claim/.
5. US Food and Drug Administration. "Medical Devices: Cybersecurity." www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm.

Joe Gillespie (joe.gillespie@tw-Security.com) is senior privacy/security consultant, and Susan Lucci (susan.lucci@tw-Security.com) is senior privacy/security consultant and privacy officer at tw-Security.

Article citation:
Gillespie, Joe, Susan Lucci. "Avoid Pain After a Breach—Read the Fine Print." *Journal of AHIMA* 90, no. 6 (June 2019): 30-31.