Global Knowledge®

Expert Reference Series of White Papers

Healthcare Organizations and Data Breach: How to Lower Risk and Reduce Liability

Healthcare Organizations and Data Breach: How to Lower Risk and Reduce Liability

David Willson, JD, LLM, CISSP, Security+

Healthcare Breach Statistics

In light of the recent Anthem breach it seems fitting to discuss what healthcare organizations can and should do to protect healthcare records, lower the risk of a breach, protect their reputation, and reduce their liability. Most of us only hear about the very large and public data breaches, like Anthem. Make no mistake, the Anthem breach is just the tip of the iceberg and should be a huge wakeup call. But, it is in no way an isolated event when it comes to breaches against healthcare organizations. Since 2009, data on more than 120 million people has been compromised in breaches on more than 1,100 organizations.[1] "2015 is already the year of the health-care hack — and it's only going to get worse."[2] In addition to Anthem here are some other relatively high-profile healthcare breaches you may have heard about: Premera Blue Cross, Seton Healthcare Family, MetroHealth Hospital, In Compass Health, and CareFirst BlueCross BlueShield (1,100,000 affected). Some of the 60- plus smaller reported breaches (hacking, theft, loss, unauthorized access, and more) for 2015 include: Alexian Brothers Medical Center (632 affected), Associated Dentists (4,725 affected), Duke LifePoint Conemaugh Memorial Medical Center (1,551 affected), Ventura County Health Care Agency (1,339 affected), Jacobi Medical Center (90,060 affected), Bellevue Hospital (3,334 affected), EyeCare of Bartlesville (4,000 affected), Pediatric Associates (627 affected), Elizabeth Kremer, M.D. (873 affected), and the list goes on and on.

Ninety percent of firms participating in a recent Ponemon Institute healthcare data security study indicated having been breached, and 40 percent suffered more than five breaches over the last two years.[3] "There is a perception that, because of limited resources, healthcare does a poorer job than other sectors in managing cyber risk."[4]

Why Should You Be Concerned?

A recent Ponemon Institute survey reveals that, "for the first time, criminal attacks are the number-one root cause of healthcare data breaches."[5] "Cyber criminals recognize two critical facts about the healthcare industry: 1) healthcare organizations manage a treasure trove of financially lucrative personal information and 2) they do not have the resources, processes, and technologies to prevent and detect attacks and adequately protect healthcare data."[6]

---

[1] Peterson, Andrea, "2015 is already the year of the health-care hack — and it's only going to get worse," Washington Post (20 Mar. 2015).
[2] *Id.*
[3] Greenwald, Judy, "Cyber criminals widen scope of industries to attack," Business Insurance (25 May 2015), citing the Ponemon Institute study, "Criminal Attacks: The New Leading Cause of Data Breach in Healthcare."
[4] *Id.*
[5] "Criminal Attacks: The New Leading Cause of Data Breach in Healthcare," Ponemon Institute (7 May 2015).
[6] *Id.*

The reality is that the healthcare industry and those who have access to or hold protected health information (PHI) have been identified as prime targets and the attacks are becoming more and more sophisticated. The Anthem breach was very sophisticated, or at least that is what the initial reports indicate.[7] Some believe it was either an inside job by an employee who had or who stole credentials, or was the result of a phishing attack wherein hackers stole credentials.[8] The data included "names, dates of birth, member ID/Social Security numbers, addresses, phone numbers, email addresses and employment information such as income data."[9] Regardless of whether it was an insider or hackers, the attack appears to have been very sophisticated. Some believe the Chinese were responsible.

In 2014 the FBI warned healthcare organizations that their security is lax and that they are vulnerable to cyber-attacks. "The healthcare industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely . . . ."[10] Healthcare information provides the necessary data to create profiles for financial theft, access to bank accounts, as well as to impersonate patients and obtain controlled substances.[11]

Impact to Your Reputation

"For the people whose data was compromised in the Anthem breach (or the Target breach, or the RSA breach, and on and on) it matters little who acquired their data or even how it was acquired. What matters most is that an organization they trusted with their data didn't do enough to protect it."[12]

Consumers/patients don't care why or how you were breached. Their only concern is what you are doing to fix it and why you let this happen. Companies that don't react quickly and satisfactorily usually end up being crucified in the media. Due to the recent number of breaches, many consumers/patients are ready to pull the trigger on a lawsuit as soon as a public announcement acknowledging the breach is made by a company. The first lawsuit against Anthem was filed within 24 hours of the public announcement acknowledging the breach.[13] Not even enough time for Anthem to explain themselves.

Some organizations, presumably in a panic and lacking all the facts, initially deny a breach has occurred. Later, when it is confirmed, they are forced to acknowledge the breach. Rather than reserving comment of facts, some then claim very few records were impacted. In the end these organizations lost a lot of credibility and had to admit that their statement about the number of records impacted was incorrect. For instance, when the Utah healthcare system was breached, initial reports were a few hundred thousand records exposed. Final count was three quarters of a million records, with a current cost to the state of about $9 million.[14] More recent is the IRS breach. The IRS commissioner, Mr. Koskinen, stated, "This is not a hack or data breach. These are impostors pretending to be someone who has enough information to get more."[15] If you are one of the 100,000-plus whose tax information was stolen, does it matter to you how the IRS wants to label the theft? Does his statement allay your fears and frustration or just make you angrier that they did not protect your information?

---

[7] "Anthem hack affected millions of noncustomers," BusinessInsurance (Reuters) (25 Feb. 2015).
[8] *Id.*
[9] *Id.*
[10] Finkle, Jim, "Exclusive: FBI warns healthcare sector vulnerable to cyber-attacks," Reuters (23 April 2014).
[11] *Id.*
[12] Kearns, Dave, "How We Can Prevent Another Anthem Breach," DarkReading, 18 Feb. 2015.
[13] Ellison, Ayla, "Anthem hit with class-action lawsuits less than 24 hours after announcing data hack," Becker's Hospital Review (6 Feb. 2015).
[14] Stewart, Kirsten, "Report: Utah's health data breach was a costly mistake," Salt Lake Tribune (28 May 2015).
[15] McKinnon, John D., and Saunders, Laura, "Breach at IRS Exposes Tax Returns - Thieves used agency's online services to get information for about 100,000 households," The Wall Street Journal (26 May 2015).

The best way to protect your reputation is to appear as though you have taken control of the situation, are taking responsibility, are not attempting to blame others, and are putting the needs and security of the consumer/patient first. We all understand that mistakes happen and that defending against sophisticated attackers can be near impossible. It is how you handle the breach that will make a difference. You likely cannot prevent most breaches, but being able to demonstrate that your security was reasonable and your organization's reaction was forthcoming and in the interests of those impacted will go a long way to help your case.

Compliance is Not Good Enough

Compliance is the law and it is a must. Unfortunately ensuring your organization is HIPAA compliant is not going to save you. Compliance does not equal security. Yes, compliance will help you avoid fines, but you will continue to get breached and thus patients will sue and your reputation will suffer.

What Can You Do?

Healthcare organizations need to take a closer look at how they are managing this problem, or I should say risk. The entire environment has changed and most companies and organizations, not just healthcare organizations, have been slow to adjust. Healthcare data has always been valuable, but when it was merely on paper and locked up it was not readily available in such huge quantities. Now that it is in electronic form and virtually everywhere and anywhere, its value has risen exponentially due to its availability. The question therefore becomes, how do you make the information you need and patients want, conveniently available to healthcare providers and patients alike, while at the same time keeping it out of the hands of those seeking to take it for nefarious means?

Well, there is bad news and some good news. The bad news is there is no silver bullet. There is no piece of hardware, software, tool, procedure, technique, etc., that will protect this data, despite what many vendors will subtly try to convince you. Also, the government does not have the answer. As is evident from the recent IRS breach and many other government breaches, they are in the same boat. HIPAA compliance, as stated above, will not make your organization more secure, it will make you compliant and that is it.

Finally, cyber insurance, which is a must, is not the silver bullet either. It is one layer of protection for when all goes south. Relying completely on cyber insurance, like some companies do, is like driving blindfolded and claiming that it is okay because you have car insurance. Simply negligent.

The good news: organizations can start now by understanding the risks and vulnerabilities; utilizing good hardware, software, procedures, techniques, training, etc.; and putting a comprehensive plan in place to protect data while at the same time preparing for the inevitable data breach. Preparation will allow organizations to detect and react quickly. Today most organizations are in a reactive mode and that is, unfortunately, how detection software works—reacting to threats. Put a plan in place now to lower the risk and enable your organization to react quickly in the event of a breach. This is one of the few proactive steps organizations can take.

Steps Organizations Can Take to be Better Prepared

In order to lower the risk of a breach, ensure compliance, reduce or eliminate the liability when breach is discovered, protect the reputation of the company, and react and recover quickly, there are three basic steps healthcare organizations can and should take. These are not tasks to be assigned to IT or someone from the mail room. These tasks are specifically for the leadership, the executive team—those in charge and responsible for the organization. Cybersecurity and data breach are NOT an IT issue but a management issue. Even if you hire an outside organization to do this, the leadership must be fully engaged. It is your organization, you have a fiduciary responsibility to protect it.

- **Step 1**: Understand the Data Your Organization Collects
  The first step is to understand what data your organization collects, processes, and stores. For instance: how the data is collected; where it goes once its collected; and who has access to it (within the organization and outside of it). Then, determine how this data is being secured. Annotate what measures, tools, techniques, and procedures are used and implemented to keep data secured. All data should be classified based on its sensitivity. If it is public data, don't worry about securing it. If it is sensitive patient data, personal data, social security numbers, addresses, etc., protect it and limit access to those with a need to know.

- **Step 2**: Create a Security Policy and Inform Your Organization
  The second step is to draft the policies that outline your security plan, and inform employees and vendors what their responsibilities and obligations are for protecting this data. Remind them that this is not just patient, consumer, or client data, but their personal data as well. Human resources holds all of the data on employees and most don't realize that their actions may not affect just patients but their own personal data as well. Contracts and/or agreements with vendors must ensure that they are taking the security of your data seriously and require them to implement a good security program satisfactory to your needs.

- **Step 3**: Keep Everyone Informed Through Training
  The third step is to train, train, and train. Once the plan is in place and policies are written, train ALL—to include the leadership, doctors, nurses, vendors, and all employees—on the security procedures, how data is lost and stolen, risks, vulnerabilities, and their responsibilities for protecting all data. Make the training personal. If data is lost or stolen it obviously impacts the patient, but also the organization, individual jobs, and potentially employee personal data, jobs, and personal life.

Cyber Insurance

As stated above, cyber insurance is a great tool and highly recommended. When considering insurance, though, do your homework. Some significant issues have arisen with regard to insurance coverage after data breaches. First of all, make sure to fully understand what is included in the coverage. In some cases, the organizations believed the policies covered the incidents only to find out that they did not. For instance, in *Recall Total Information Management, Inc. et al. v. Federal Insurance Co. et al*, the insured, Recall, sued Federal Insurance Company for coverage after the loss and theft of 130 storage tapes. The tapes, which contained the personal data of more than 500,000 current and former IBM employees, fell off the truck transporting them and disappeared. The plaintiffs, Recall, sued claiming the incident was a personal injury loss due to the personal information on the tapes, and a property damage loss. "The Connecticut Supreme Court agreed with an appellate court that the loss of the computer tapes did not constitute a personal injury as defined by the policies, because there had been no publication of the information that violated the privacy rights."[16] Had the personal information on the tapes been published and/or one of the individuals whose data was on the tapes suffered identify theft there may have been a different result for the plaintiffs.

[16] Greenwald, Judy, "Court Rules for Insurers In Case of Data That Fell Off Truck," Business Insurance (25 May 2015).

As applications for insurance are submitted, organizations should ensure that the assertions made are accurate and are maintained throughout the life of the policy. For instance, failing to implement or maintain "adequate," "reasonable," or "minimum required practices," with regard to security may result in the denial of a claim. In *Columbia Casualty Co. (CNA) v. Cottage Health System*, a lawsuit was filed after CNA claimed that "Cottage Health failed to 'continuously implement the procedures and risk controls identified in its application,'" violating the, "Failure to Follow Minimum Required Practices," clause of the policy, which led to the breach of healthcare data involving 32,500 individuals.[17] CNA claims that Cottage Health attested to a certain level of security and failed to maintain that level. They are accused of failing to replace default settings and implement secure configurations, and failing "to regularly check and maintain security patches on [their] systems . . ."[18] The policy specifically holds that it "shall be null and void if the Application contains any misrepresentation or omission . . . which materially affects either the acceptance of the risk."[19]

Any policy, especially if it provides coverage in the event of a data breach, privacy breach, or some other cyber incident, should be reviewed by individuals with the requisite expertise for the issues and coverage. For instance, a data breach or some other breach of information will most assuredly involve many technical issues. Therefore, someone with the technical knowledge of the security for the organization should be involved in a review. Others may include someone with knowledge of insurance terms and policies, and someone with a technical understanding of the network and implementations, potential risks, legal issues, etc.

Conclusion

The time for assuming or pretending that a data breach will not happen is long gone. All will, many have, and many will continue to suffer data breaches. This is a threat that can no longer be ignored. You can no longer claim you don't have the budget. Deciding to delay taking action until next budget cycle could potentially be considered negligent. This responsibility cannot be ignored and it cannot be outsourced. The level of attention and involvement the leadership of the organization, to include physicians, put toward this problem is in direct relation to their level of liability after a breach. Ignore it and your level of liability is astronomical. Take an immediate active role and the liability is reduced significantly. It is much more costly, monetarily as well as with regard to your reputation, for an organization to react to a breach rather than planning for it.

[17] Anderson, Roberta, "The devil in the cyber insurance details," Advisen Cyber Risk Network (28 May 2015). *See* also, Greenwald, Judy, "Cyber claims start heading to court," Business Insurance (25 May 2015).
[18] Anderson, Roberta, "The devil in the cyber insurance details," Advisen Cyber Risk Network (28 May 2015).
[19] *Id.*

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge through training.

- CompTIA Healthcare IT Technician Certification Prep Course (HIT-001)
- HCISPP Certification Prep Course
- Cybersecurity Foundations
- CyberSAFE (Securing Assets For End-Users)

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

David is an attorney and an expert liability management and cybersecurity consultant, licensed in NY, CT, and CO. He helps companies understand the liability associated with information security and data breach. He also assists law firms with technical litigation, electronic evidence discovery, and the introduction of this evidence. He has worked in information security for more than 15 years and has written and provided lecture in this area over the last three years. David is a retired Army JAG officer. During his 20 years in the Army he provided legal advice in computer network operations, information security, and international law to the DoD and NSA and was the legal advisor for what is now CYBERCOM. He has published many articles, spoken at many conferences, and conducted numerous classes and training in risk management.