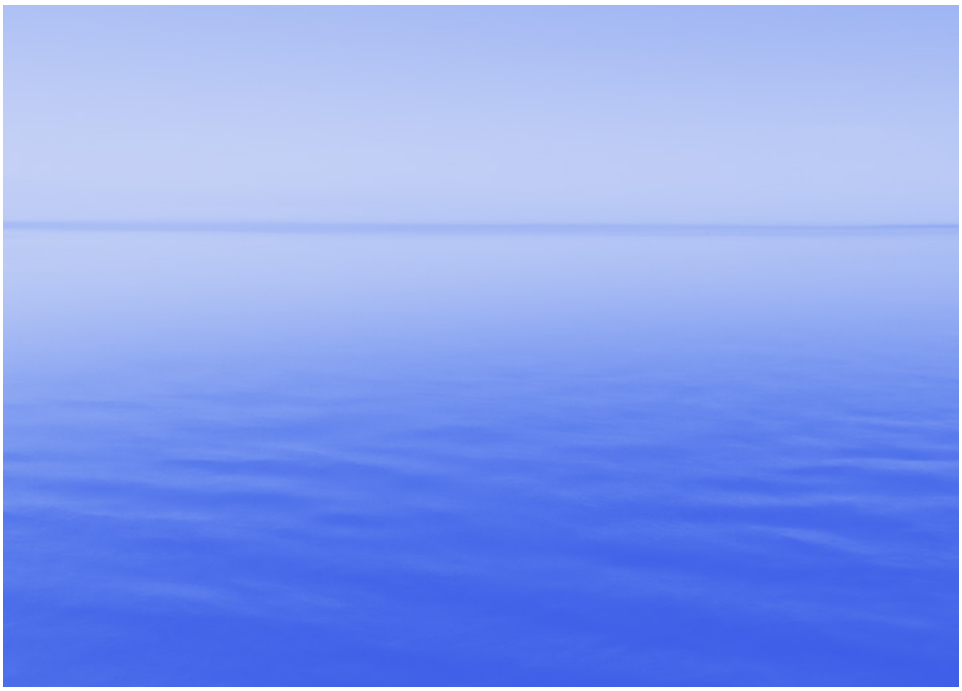
Clearwater

Whitepaper

10 Ways Business Associates Can Turn Their HIPAA Compliance and Cybersecurity Program Into a Competitive Advantage

Table of Contents



Introduction

Managing vendor risk is challenging, especially when it comes to cybersecurity and Health Insurance Portability and Accountability Act (HIPAA) compliance.

If you're a vendor working in the healthcare industry (classified as a "Business Associate" under HIPAA), an effective HIPAA and cybersecurity program isn't just good for business, it can help you stand out among your competitors and potentially save you money by decreasing the chance you'll be hit by penalties and ensuring you land new business quickly and with confidence.

Why is HIPAA compliance and cybersecurity important for healthcare vendors?

In 2018, attackers hit American Medical Collection Agency (AMCA), a medical bill and debt collector. The breach resulted in theft of data that affected AMCA clients including LabCorp and Quest Diagnostics.

Some reports indicate more than 20 AMCA clients are affected, resulting in the breach of an estimated 25 million patient records—almost 8 million from LabCorp and another almost 12 million from Quest.

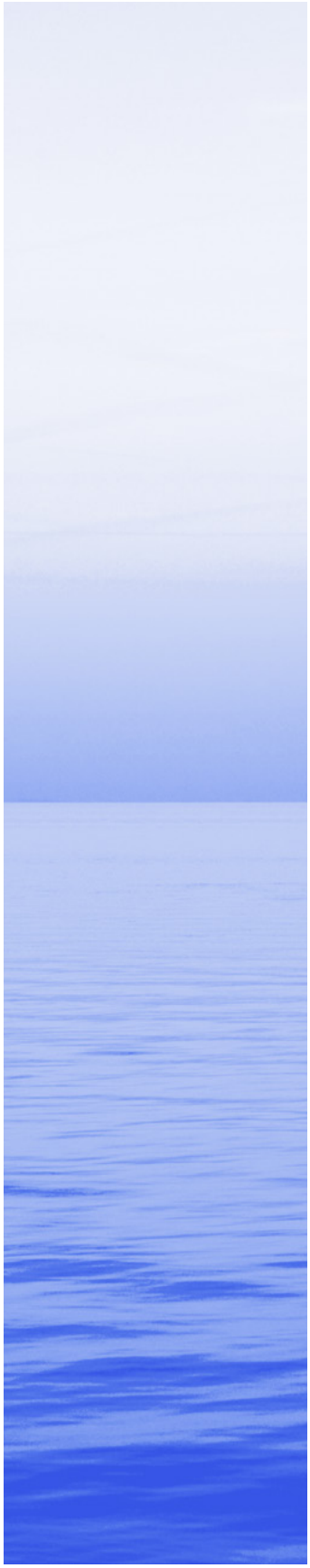
Stolen among the data was personal information such as credit card numbers, Social Security numbers, bank account information, addresses, birth dates, names, and some medical information.

Although the hack of the vendor began in August 2018, it wasn't discovered until March 2019—some eight months later.

Within months, AMCA filed for Chapter 11 bankruptcy, citing costs related to the breach as a driving factor.

The bankruptcy filing means clients like LabCorp and Quest are left to deal with the fallout. They had to notify their customers of the breach. They'll shoulder the expense of credit checks and credit monitoring for affected clients, and they'll likely be on the hook for class action lawsuits related to the breach.

To date, the AMCA breach is the second largest data breach of patient information, following the staggering loss of nearly 80 million records during a 2015 breach that affected Anthem.



Costs of managing vendor risks

Managing risks associated with vendors is an increasingly pressing issue for healthcare cybersecurity.

While the AMCA breach was among the most costly in 2019, it's only a portion of the total cost of data breaches in healthcare. The estimated cost of healthcare data breaches last year that accessed patient personal information was nearly $4 billion.

In the first two months of 2020, more than 30 data healthcare industry data breaches were reported, affecting more than 1 million patients. If patterns continue, industry experts won't be surprised to see 2020 breach-related expenditures meet or exceed 2019.

And the related cost of these breaches isn't chump change for organizations.

In the U.S. healthcare industry, breach-related costs average at about $429 per record, the highest per record cost for a breach of any industry in the world. The average size of a data breach is 25,575 records. At $429 per record, that means an "average" breach could cost your organization about $11 million, but as you can see from examples we've talked about, many breaches far exceed those numbers.

Unfortunately, when these breaches happen, liability doesn't always shift to the vendor, even with vendor agreements in place.

Who's responsible?

If you're a vendor, or you're an organization contracting with an outside vendor, you may be uncertain where liability falls.

Many organizations believe if they have a business associate agreement with a vendor, that's good enough.

Close, but not actually.

> The AMCA data breach of 25 million patient records is the second-largest ever healthcare data breach.

As a covered entity, a healthcare provider could permit a business associate to create, receive, maintain or transmit electronic protected health information (ePHI) on its behalf, but only if the organization gets satisfactory assurances the business associate will properly safeguard that data.

In most instances, that means getting assurances in writing.

However, many organizations don't have business associate agreements at all. Sometimes that's because the vendor and covered entity have worked together for years or maybe it's because a new vendor wasn't acquired through traditional acquisition processes.

Whatever the case, a business associate agreement is a key part of any covered entity's HIPAA compliance and cybersecurity objectives.

Third-party risk is an increasing concern for healthcare providers and vendors alike.

If you're a vendor contracting with a healthcare provider, your concerns often include challenges meeting customer expectations as well as related costs. These concerns often create friction for organizations attempting to manage vendor risks. To further complicate matters, expectations are changing and becoming more in-depth.

For example, healthcare providers should expect their vendors to have a cybersecurity program in place and that the vendor can answer related questions about the effectiveness of that program.

There's also increasing pressure to ensure vendors meet HIPAA security and privacy requirements, and can manage compliance and cyber risk concerns on an ongoing basis.

Global healthcare providers spend, on average, about $3.92 million each year to manage vendor risk. For the industry as a whole, third-party risk expenditures almost reach $24 billion each year.

Challenges for healthcare cybersecurity programs

While many healthcare organizations may agree that HIPAA compliance is paramount and a robust cybersecurity program is a must, the reality is the industry, as a whole, has many challenges when it comes to effectively building and maintaining these programs.

From a shortage of trained, qualified professionals, to a lack of funding and executive support, many organizations just don't have the people, processes and tools they need. Because of these limitations, organizations often get bogged down trying to understand the requirements or buying expensive tools in an attempt to find quick fixes instead of establishing the fundamental governance structure and implementing the processes that are necessary to achieve the objectives that are demonstrable of effective compliance and cybersecurity programs.

So, if you're a vendor, how can you ensure you're not only meeting cybersecurity and compliance requirements, but you're also quickly closing new opportunities and mitigating unexpected expenses and delays related to cybersecurity and compliance inefficiencies?

> Vendors and business associates with strong cybersecurity and HIPAA compliance programs have a distinct advantage over other vendors vying for opportunities to work with covered entities.

Here are 10 ways business associates can turn HIPAA compliance and cybersecurity program into a competitive advantage:

1. Set privacy and security risk management and governance program in place

Like building a house, your risk management, cybersecurity program, and HIPAA compliance programs should begin with a solid framework.

When it comes to compliance and cybersecurity, there are a variety of existing frameworks from which you can build.

One example is the NIST Cybersecurity Framework. Intended for organizations in critical infrastructure industries, such as healthcare, this framework lays out the security objectives and activities an organization should adopt as part of a comprehensive program. It also provides references to standards, best practices, and guidelines to assist organizations in understanding how to best execute the identified activities. Perhaps best of all, this framework is free to any organization and available along with supporting documents on the NIST website.

When using the NIST Cybersecurity Framework or any other framework, be sure to map your organization's requirements, including the HIPAA requirements, into your organization's target profile. While unofficial, the Office for Civil Rights (OCR) has mapped the HIPAA Security Rule requirements to the NIST framework and made the mapping publicly available. It's a great way for all organizations, regardless of size or budget, to adopt a framework to start and build out your program as it matures over time.

2. Develop and implement HIPAA privacy, security, and breach notification policies and procedure

After picking your framework and creating a target profile, you'll need to begin implementation. This should include developing and implementing HIPAA privacy, security, and breach notification policies and procedures.

At a minimum, you should include all the policies and procedures required for your organization's compliance.

Not sure where to begin? Many organizations have HIPAA policy and procedure templates you can use to ensure you meet those strict requirements.

3. Train all members of your workforce

Next, it's important to educate team members throughout your organization about your programs so they understand the policies and procedures you've created.

Some policies and procedures will be applicable to everyone. Some will be applicable only to specific people or job functions. With appropriate training, you can help your team members understand what they're expected to do, when they need to do it, and how to handle their related roles and responsibilities. Make sure the right people get the right information they need to facilitate compliance and cybersecurity success.

4. Complete a HIPAA security risk analysis

It's important to understand where you have risks within your organization's IT ecosystem, what those risks are, and how significant they may be.

As part of HIPAA requirements, your risk analysis should include all of the systems used to create, maintain, receive, or transmit ePHI.

But don't forget to include your non-HIPAA related operational systems such as your finance software or human resources solution. These and similar systems are critical for your operations, so you should clearly understand all the risks associated with their operations.

Make sure as you identify threats and vulnerabilities to your systems, you understand the likelihood of the threats acting on the vulnerabilities and the potential impact to your organization if that were to happen, the existing and potential controls that are and could be used to mitigate those risk by either reducing the likelihood or impact. This will help you prioritize your efforts to manage your risks.

Here's an example: Let's say Company A uses a third-party vendor to process insurance claims. A lot of ePHI will be exchanged between Company A and the claims vendor. If you're the vendor, you'll need to have sufficient security controls in place to give Company A a level of comfort that the risk to them and their patients is acceptable before they will contract with you. Typically, Company A will send the vendor a survey or questionnaire to understand their risk. If the vendor has done a comprehensive risk analysis, they are in a position to promptly and effectively respond to that portion of the survey.

5. Address HIPAA security risk management

Once you've completed your risk analysis and know what and where your risks are, you need to treat those risks. There are several options including accepting, avoiding, transferring or mitigating each risk. In most cases, you will look to mitigate risks. This involves selecting and implementing controls that reduce the risks to levels that are acceptable for your organization. As mitigating controls are selected, decisions will need to be made on who will be responsible for implementing the controls, who will handle specific tasks during implementation, and when the implementation will be completed. It's important to track your mitigation and remediation progress and follow-up as this is both a best practice and required under the HIPAA Security Rule.

6. Complete a HIPAA security evaluation

Next, you should have a HIPAA non-technical evaluation performed. When a HIPAA non-technical evaluation is conducted, the evaluator looks at how well your organization has done in adopting security policies and procedures as required by the HIPAA Security Rule. During this examination, the evaluator may discover gaps in your security program. The gaps represent areas where your organization can continue to improve in implementing your HIPAA compliance and security programs.

7. Complete technical testing of your environment

After completing a non-technical review of your HIPAA security, you should also tackle technical testing. Unlike the non-technical evaluation that focuses on policy and procedures, technical testing will help you to discover whether or not you have weaknesses within your existing IT infrastructure and applications.

For example, you could do vulnerability assessments, penetration testing, and web application testing. During these tests, you're assessing the existing technical and, in some cases, physical controls of your systems and infrastructure. Just as with the non-technical evaluation, weaknesses and vulnerabilities identified during testing should inform future risk analysis.

Don't forget the importance of routine re-testing to ensure your processes and controls work as you designed and you don't have any new vulnerabilities within your system.

Leading organizations now include anti-phishing campaigns as part of their technical testing program. Unlike traditional technical testing that looks for technical

vulnerabilities, anti-phishing campaigns assess how vulnerable your workforce is to email-based social engineering attacks. Currently this is the most common method bad actors use to introduce malware into healthcare organizations, and identifying opportunities for and providing additional training can be a very effective risk reduction investment.

8. Implement a strong, proactive business associate management program

After completing technical testing, it's time to evaluate the risks associated with your business associates. If you're a vendor, you may also work directly with other vendors. That means, just like the organizations you work with who put you through risk assessments, you should do the same with your own vendors.

Understand related risks of working with each vendor. Be sure you have a vendor management program so you can evaluate those risks and make decisions on whether the risk level is acceptable to your organization. If not, you can always seek a new vendor and complete additional assessments until you find the one that most accurately meets your risk mitigation requirements. Also, consider if you need to have a business associate agreement in place with the vendor as required by HIPAA.

9. Complete Privacy Rule and Breach Rule compliance

It's important to understand to what extent you need to manage privacy. Know where you are relative to your applicable HIPAA Privacy and Breach Rules requirements. There are significant potential financial penalties associated with breaches much of which may be avoided or reduced if you are compliant with applicable laws and regulations including HIPAA.

10. Document and act upon a remediation plan

Rinse and repeat. This is an ongoing program. You should continuously document your progress, create and maintain a remediation plan, and follow through. These steps will help strengthen your program over time.

References:

https://healthitsecurity.com/news/46500-austin-pathology-patients-added-to-amca-data-breach-victims

https://techcrunch.com/2019/06/05/labcorp-records-stolen-quest/

https://www.advisory.com/daily-briefing/2019/08/13/data-breach

https://www.synopsys.com/blogs/software-security/cost-data-breach-2019-most-expensive/

https://securityboulevard.com/2020/01/u-s-healthcare-data-breach-cost-4-billion-in-2019-2020-wont-be-any-better/

https://www.natlawreview.com/article/over-30-data-breach-incidents-health-care-reported-to-hhs-thus-far-2020-affecting

https://www.healthcarefinancenews.com/node/138943

https://www.hipaajournal.com/2019-cost-of-a-data-breach-study-healthcare-data-breach-costs/

https://www.hipaajournal.com/2019-cost-of-a-data-breach-study-healthcare-data-breach-costs/

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Vendor opportunities

Creating robust cybersecurity and HIPAA compliance programs helps you differentiate your business from other vendors. With these programs in place—and maturing—you can demonstrate to covered entities that you can respond promptly and positively to security questionnaires and you have everything you need for great business associate agreements.

These steps can help you show potential customers that if they work with you, there are reduced risks compared to competitors.

The ClearAdvantage™ Program for Business Associates can give you a competitive edge when it comes to creating your privacy and security programs. Clearwater can help you create, implement, and improve your programs including risk management and governance, policy and procedure development, risk analyses, compliance assessments, gap analyses, risk remediation, scanning and reports, pen testing, and more.

Clearwater is the leading provider of Enterprise Cyber Risk Management and HIPAA compliance software and consulting services for the healthcare industry. Our solutions enable organizations to gain enterprise-wide visibility into cybersecurity risks and more effectively prioritize and manage them, ensuring compliance with industry regulations. Clearwater's suite of IRM|Pro® software products and consulting services help healthcare organizations to avoid preventable breaches, protect patients and their data, and meet OCR's expectations, while optimizing cybersecurity investments. More than 400 healthcare organizations, including 64 of the nation's largest health systems and a large universe of business associates that serve the industry, trust Clearwater to meet their information security needs.

Have questions regarding this white paper? Engage with Clearwater for a specific discussion about your organization's approach.

- ClearwaterSecurity.com/Contact