Clearwater

Whitepaper

Understanding Vendor Risks and How to Manage Them

ClearwaterSecurity.com

Healthcare—Secure, Compliant, Resilient

Table of Contents

Introduction

When attackers infiltrated the American Medical Collection Agency (AMCA), a medical bill and debt collector in 2019, some 25 million patient records were exposed in the second-largest ever healthcare data breach.

And while AMCA filed bankruptcy as a result, other companies like LabCorp and Quest Diagnostics are still dealing with the aftermath, carrying the financial burden and tarnished reputations.

The AMCA breach is an example of a growing number of recent data breaches that highlight just how vulnerable some third-party vendors can be.

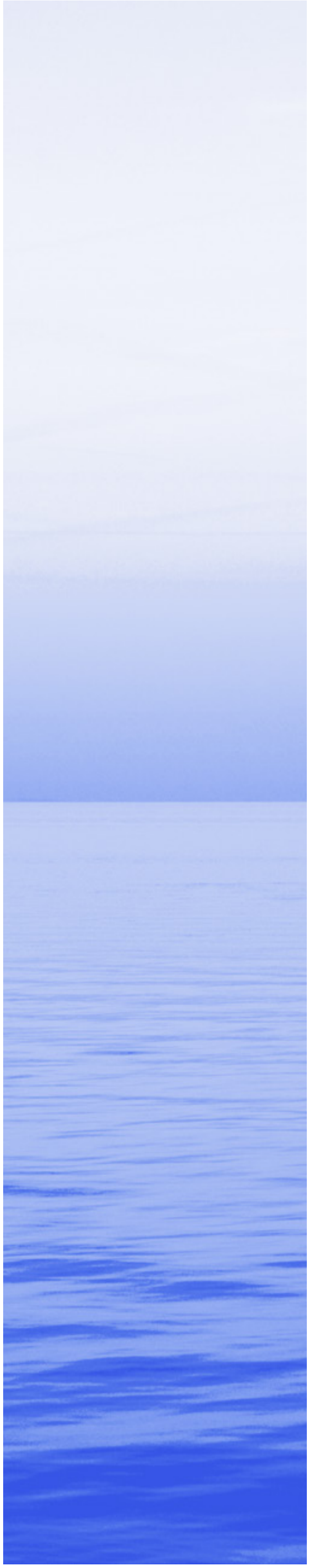
And that means you're vulnerable, too. That's because you're only as secure as your riskiest vendor.

Like these companies, you could be left dealing with financial fallout in the millions if your data lands in the hands of attackers because of a third-party breach.

So where do you begin? How do you keep your data safe with the growing number of third-party vendors that organizations of all sizes now use for day-to-day operations?

If you're unsure, you're not alone. Many healthcare organizations grapple with vendor risk management as part of the business associate requirements for covered entities. Unfortunately, as tech usage expands and becomes more intertwined with your operations, the greater the likelihood you could fall prey.

> According to a report from Ponemon Institute, almost 60% of respondents said they had one or more third-party data breaches within the last two years. That's why ensuring your vendors adhere to the same data privacy and compliance standards as your internal operations is paramount.



Regulatory agencies set the stage for compliance

As a healthcare organization, you're likely well-versed in the data privacy and data protection mandates you must meet through the Health Insurance Portability and Accountability Act (HIPAA).

If you're a covered entity, you may work with third-party vendors (business associates) that can create, receive, maintain or transmit electronic protected health information (ePHI). Under HIPAA, you need assurances these third-party vendors will safeguard your ePHI.

Your business associate agreement should outline permitted and required ePHI usage, as well as safeguards your third-party vendors use to prevent unauthorized use or disclosure of ePHI.

Healthcare organizations should routinely review HIPAA policies and practices for all of your business associates, not just when establishing new contracts, but throughout your relationship and at contract renewals.

But who do you work with that could be considered a business associate? Here are a few examples of these third-party vendors:

- Companies that handle billing, claims or collections on your behalf, for example a billing agency or a collection agency
- Document storage companies or document shredding agencies
- Accreditation organizations
- Medical transport companies
- Medical transcription companies
- Answering services
- Legal services
- Payment processors
- Health plan administrators
- Auditors or CPAs
- Consultants
- Pharmacy benefits managers
- Electronic health portals where patients access their PHI

HIPAA also outlines that if you, as a covered entity, know your business associate has a data breach or has violated your associate contract or agreement, then you have to take steps to resolve the breach or end the violation. If you can't, you're expected to terminate your contract or arrangement with that associate.

HIPAA data breaches

What happens if your vendor has a HIPAA data breach? Let's look at an example with Mercy Health-Lorain Hospital in Ohio. Mercy Health used a third-party vendor, RCM Enterprise Services, for patient billing.

In November 2019, RCM Enterprise Services, a billing and accounts receivable vendor, discovered invoices were sent to patients with the wrong information. The invoices should have displayed names, addresses, and zip codes. Instead, the invoices featured names, addresses and Social Security numbers, which were visible through address windows on envelopes. The improper documents were processed between August and October 2019.

RCM has agreed to offer those affected credit monitoring and identity monitoring and restoration services. While there have not yet been reports of any financial penalties for this data error, other cases that the Office for Civil Rights (OCR) has investigated for third-party data breaches have resulted in fines totaling millions of dollars.

FTC

While HIPAA gets much of healthcare's attention, other regulatory agencies and laws can affect your third-party relationships.

The Federal Trade Commission, for example, focuses on preventing companies from engaging in unfair or deceptive practices related to commerce. That can include healthcare organizations' Notice of Privacy Practices (NPP).

While HIPAA requires covered entities to distribute NPPs that clearly explain individual rights related to PHI and related privacy practices, the FTC can get involved if your NPP implies deceptive practices for your consumers.

How? Here's an example.

In 2010, the pharmacy chain Rite Aid settled charges with the FTC that it violated federal law by not protecting customer and employee financial and medical data. The FTC said Rite Aid used open dumpsters to discard trash with personally identifiable information (PII) – for example, job applications and prescription labels.

The FTC said Rite Aid not only improperly disposed of personal information, but it also failed to properly train employees, had not assessed its compliance related to disposal and procedures, and didn't use reasonable processes to discover or remedy risks related to personal information, even though the company made assurances it respected and protected privacy. The FTC said that claim was deceptive and its security practices were unfair.

In related actions, Rite Aid also agreed to pay HHS $1 million for violating the HIPAA Privacy Rule.

Other agencies

In addition to HIPAA and the FTC, all 50 states have legislation that require organizations to notify people of ePHI and PII data breaches.

The General Data Protection Regulation (GDPR) went into effect in 2019 and regulates data protection and privacy in the European Union, including transfer of personal data outside of the EU and European Economic Area. In Germany, for example, through GDRP a hospital was fined for sending invoices to the wrong patients. Those incorrect invoices contained PHI for other patients.

Vendor risk. Always. Everywhere.

So when do you have risks from your vendor relationships?

The answer is always.

Here are some of the ways you incur risks from your vendors:

Operational risks

On average, organizations experience about six outages each year related to critical business systems including patient care systems.

Security risks

Thousands of users can connect in to a third-party vendor and sometimes they can have full access to your network with shared credentials.

Financial and reputational risks

According to the 2019 Cost of a Data Breach study conducted by the Ponemon Institute, the average cost of a healthcare data breach is $6.45 million. And studies have shown that it can take 10 months to more than two years to restore an organization's reputation following a breach of customer data.

Compliance and regulatory risks

As we previously mentioned, for HIPAA, organizations are responsible for securing vendors that have access to regulated data or systems. If your third-party vendor has a violation, you can be fined, have operational limitations, and face civil and criminal liabilities—even if vendor caused the breach.

Challenges working with third-party vendors

When you work with third-party vendors, their risks are your risks.

According to Ponemon Institute's Economic Impact of Third-Party Risk Management in Healthcare Report, almost 60% of respondents indicated they have had one or more third-party data breaches in the past two years. The average cost of the vendor-related data breaches is just shy of $3 million.

Respondents indicated that have difficulty managing third-party vendors, especially because many healthcare organizations don't use automated tools to help them with their management processes and many still rely on manual risk management processes when dealing with vendors. That lack of automation often keeps agencies lagging behind cyber threats that target the industry.

Increased security complexities

Dealing with third-party vendors for data security and protection is also challenging because it's difficult to enforce compliance externally in the same way you can within your own organization and with your own employees.

Some organizations also don't have a complete and accurate list of vendors that access to their sensitive data.

Did you know that on average, companies share data with 583 third parties[1]? Without an accurate inventory, it's difficult, if not impossible, to determine how well each vendor is meeting your security requirements.

Insufficient resources

It's daunting to start a new risk management program or improve an existing one if

[1] Ponemon Institute: "Data Risk in the Third-Party Ecosystem"

you don’t have subject-matter expertise. A mature and effective risk management program requires resources that many organizations just don’t have.

Unfortunately, trained professionals are also in short supply and many organizations don’t prioritize the value of working with outside risk management professionals.

Even though the number of vendor-related cybersecurity risks are increasing, according to the Ponemon report, only 27% of respondents say their organizations conduct vendor risk assessments.

On average, healthcare providers have about 3.21 dedicated, full-time employees who do more than 500 hours of vendor risk assessments each month[2].

Outdated models

There’s a false assumption for many organizations that third parties are single-handedly responsible for doing what’s required to protect your data. Vendor risk is also often seen as something that exists on its own outside of your organization, so it doesn’t get the same priority as internal risks and issues.

This can be further complicated for organizations where siloed business units result in individual departments or work groups assessing their own vendors without standardized, organizationally directed assessment protocols. Not every team member has effective tools or proper risk assessment training, which can result in incomplete or unsophisticated assessment models.

Adoption of new vendor risk management approaches also remains low across healthcare industry.

According to the 2019 Cost of a Data Breach study conducted by the Ponemon Institute, the average cost of a healthcare data breach is $6.45 million.

[2] Ponemon Institute: “The Economic Impact of Third-Party Risk Management in Healthcare”

Data protection and risk assessment processes

Vendor risk assessments are challenging, so where do you begin? Here are a few recommendations you can put into action today and work into your existing vendor procurement and related processes:

Procurement

During your vendor procurement processes, complete security due diligence and initial vendor security assessments and approvals.

Contracting

During your contracting processes, ensure baseline security controls are included in the contract. Also make sure there is a clear understanding of what happens to your data (is it destroyed or returned to you?) when your contract ends.

Onboarding

When onboarding a new vendor, ensure the third party only gets access to the data needed for related tasks and securely set up that access. Use access controls to limit access into your network and data.

Service delivery

Conduct routine audits to ensure your vendors are meeting the requirements set forth in your agreements and contracts. Use this as an opportunity to identify and mitigate risks before a breach may occur.

Rebid/Renewals

If you're looking to continue your relationship with an existing vendor, be sure to re-evaluate each vendor's security posture before renewing. Remember, no vendor, regardless of how long you've worked together, is static. There will be changes.

Assess, prioritize, monitor, audit and re-assess. These steps help control your third-party vendor security risks and ensure your organization's data safety.

Offboarding

When your contract comes to an end, ensure your vendors meet your pre-determined conditions about what happens to your data. Get vendor certifications that they have either returned or destroyed all the data they had access to per your agreement.

Strategies to reduce vendor risk

In addition to the risk assessment processes we just mentioned, let's take a look at some of the ways you can reduce vendor risk when it comes to your PII and ePHI data.

Build a framework to assess vendor risk

First, know your vendor management lifecycle and align your risk assessment processes.

- **Contracting:** From the beginning, ensure your contracting agreement includes HIPAA and other regulatory and compliance guidelines. Remember, HIPAA requires vendor contracts to include privacy and security assurances.
- **Assessment and Prioritization:** Identify each vendor's level of access and then assign a security risk rating for each vendor based on that access. This will help you identify the most critical risks to your organization. Then prioritize vendors by risk and initiate an audit for those considered highest risk.
- **Monitor and Audit:** Monitor your vendors based on your risk assessment and which data (and how much data) the vendor accesses. For example, a vendor that accesses ePHI externally may require greater monitoring than a vendor who only accesses that information on site.
- **Re-assessments:** Conduct routine risk assessments, at a minimum at least once each year. Continuous monitoring will help you evaluate how well each vendor meets your security requirements and their effectiveness in protecting your ePHI and PII.
- **Contract termination:** As we mentioned before, don't let a third-party vendor leave with access to your data. When your contract ends, be sure your vendor has completed your requirements to either return your data or destroy it.

Implement control measures

- Analyze your vendors' security protocols to ensure you have granular levels of control for how much or how little access you give each vendor, including the specific data your vendors (and their employees and subcontractors) can see on your network.

- Keep complete control of vendor access to minimize your exposure to third-party data breaches.
- Use encryptions, firewalls, and multi-factor authorization controls to protect assets and data.
- Emphasize and require diligent password management. Require vendors to change passwords after setup during first login and do not allow reuse of old passwords.
- Make sure your vendors know your controls and what their obligations are.
- If you set internal data controls, make sure your vendors know and use the same controls.
- Include your controls and requirements into your vendor agreements so vendors know expectations.
- Once you know risks related to each vendor, you can choose to accept, refuse, mitigate or transfer those risks. If you choose to accept or mitigate, you have to take appropriate action to further protect your data.

Respond to security risks

- Vendor risk assessment is never set-it-and-forget it. You should continuously audit and monitor your vendors because risks can change. Don't forget about fourth-tier vendors.
- Conduct regular audits and assessment to evaluate security and privacy practices for each vendor.
- Implement formal evaluation processes, including your vendors' subcontractors.
- Even if you've double-checked your vendor for security practices and signed a detailed contract, remain vigilant to ensure each vendor fulfills data security obligations.
- Use technology to help you continuously monitor network and system access. Ensure that only authorized users have access to your data and that access is within the scope of your contract.
- Make sure your vendors implement and maintain your required security controls.
- Continuously monitor vendors to make sure they don't drop controls and put you at risk.

- Use in-depth report logs. Monitor the who, what, when, where, why, and how of every individual that accesses your data.
- Monitor and track all movements on your network.
- Assess for vulnerabilities.
- When you discover that your vendor has security or compliance gaps, put them on notice to remediate immediately.
- Maintain an acceptable level of risk with all of your vendors and routinely re-evaluate.

Co-existing with vendor risk

Even the best vendor risk assessments and continuous monitoring won't completely eliminate risks related to your outside business relationships.

Any time a vendor can access your systems, data, or network, there's a chance you could suffer a data breach.

Risk assessments help you determine which level of risk your organization is comfortable taking on and drives your processes to manage that risk while also planning for response and recovery in case an incident happens.

Remember, you're only a secure as your riskiest vendor, so don't delay in adopting, fine-tuning, and maturing your assessment practices and security policies.

If you'd like more information about how you can help build stronger risk assessment processes for your third-party vendors, check out our on-demand webinar, where we take a deeper dive into the business risks imposed by third-party vendors and how you can determine what's an acceptable amount of risk.

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