Clearwater

Whitepaper

The HIPAA Compliance and Cybersecurity Challenges Facing Digital Health Companies

Table of Contents

Introduction

Spurred in great part by the coronavirus outbreak of 2020, an increasing number of healthcare organizations are adopting new technologies at faster rates than ever before.

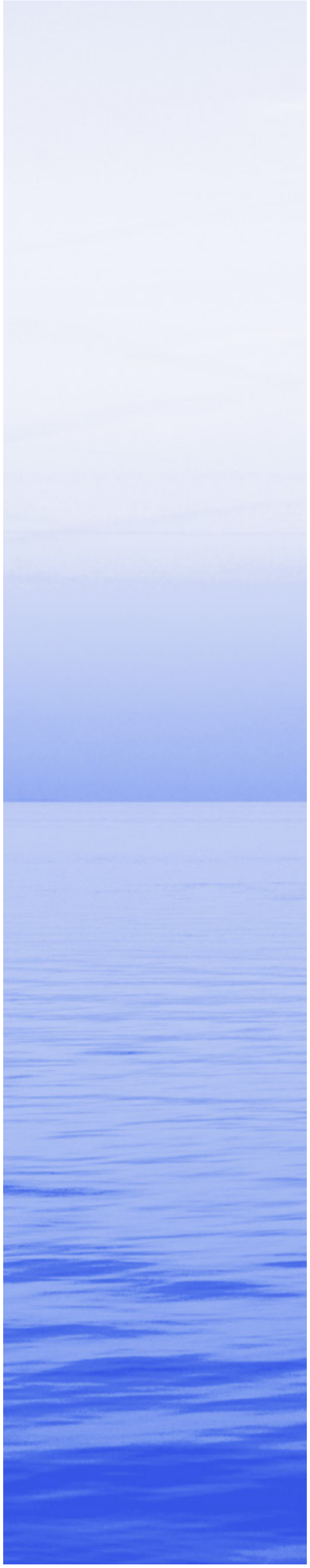
It's a trend driven by a push to meet increasing consumer needs where telehealth and remote care opportunities are front-and-center for countries around the globe tackling social distancing and stay-at-home mandates in light of the pandemic.

And while increased adoption of new technologies, applications, devices, and services certainly brings a number of benefits to healthcare organizations and patients, it also brings with it a growing list of challenges, especially when it comes to meeting HIPAA compliance mandates and other privacy and security expectations.

Not only are regulatory and oversight agencies demanding more from healthcare providers and their business associates, so are consumers, who, in light of several high-profile data breaches, want reassurances that their protected health information (PHI) and personally identifiable information (PII) is safe. They also want to know, clearly, how their data is stored, transmitted, and shared with third parties.

As this list of expectations continues to grow in both length and complexity, developers of healthcare technology are often looking at a mountain of mandates they worry may limit their growth potential.

Unfortunately, many IT vendors lack required resources and expertise to meet these increasing demands.



Current state of digital health adoption

While the ongoing digital transformation in healthcare began before the pandemic of 2020, we can see an acceleration of technology adoption across the industry since the beginning of last year. Many industry experts agree that the coronavirus outbreak is the single most disruptive event on healthcare we have experienced in our lifetimes.

In addition to a push for more telehealth options and services, we're seeing an increasing number of people in healthcare and other industries working from home. There's also an increased demand for health services delivery outside of the traditional hospital environment, especially in communities where coronavirus response has overwhelmed staff and facilities.

Looking forward at healthcare trends, it's estimated the digital healthcare market will exceed $510 billion by 2025. Much of that growth is likely to be supported by increased venture capital investments into the industry, which have seen an increased growth in funding by almost 70% in recent years.

As these growth factors contribute to the changing face of the industry as we know it, we're seeing an increased need for healthcare data access from various points – for example, between a provider and a third-party that provides services like a digital health portal where patients can review and access their ePHI.

This increased usage of third-party services introduces new risks to healthcare organizations and the consumers who use their services. We're now seeing new—and increasing numbers of—vulnerabilities we've never seen before. With these vulnerabilities come new opportunities for bad actors to target PHI, PII, and other sensitive data through a variety of attack methods—everything from vulnerability and misconfiguration exploits, to coding errors, to phishing schemes and ransomware attacks.

All of these factors are increasing risks to PHI confidentiality, integrity, and availability.

Increased attacks for healthcare

Between Jan. 1, 2020, and Dec. 31, 2020, the Office for Civil Rights (OCR) launched investigations into nearly 650 breaches affecting 500 or more patient records. Looking at data between 2019 and 2020, there's been an increase of over 25% in the number of breaches of 500 records or more.

While those numbers are already high, the reality is these are only the reported breaches that exceeded 500 or more record exposures per breach. We know there were even more breaches that affected fewer records, and potentially known unreported breaches and also other breaches that began in 2020 but have not yet been discovered.

On top of the increasing number of breaches, United States healthcare has the notoriety as the industry with the most expensive breach costs. According to a IBM's 2020 Cost of a Breach Study, that number exceeds $7 million per breach and the average time to discover and contain a breach (across all industries) is 280 days.

These breaches are not only increasing in number, but they're also increasingly complex, and as healthcare organization rely on a growing number of third-parties for technology and outsourced services—often to third-parties that handle data for multiple organizations—there's increasing likelihood that attackers can now access tens of thousands—if not millions—of records in a single successful hack.

As these breaches get more public attention—especially high-profile breaches that make national and global headlines—healthcare providers are raising their expectations regarding the HIPAA compliance and cybersecurity best practices of their IT vendors. As a result, successfully employing and managing strong compliance and security programs is paramount for healthcare technology companies. They're increasingly critical components of resilient business operations and may very well be the single most important factor about whether or not your organization succeeds and scales in the future.

Increasing expectations

Healthcare technology vendors now face an increasing list of expectations from regulators, investors, and customers including:

- Compliance with HIPAA and other regulations
- Winning new business
- Building business continuity, resiliency, and brand equity

> 56% of surveyed healthcare organizations say they had one or more third-party data breaches within the last two years.
>
> There were 230 breaches attributed to business associates accounting for 63% of breached ePHI records and 41% of them actually experienced six data breaches with vendors.

Because of the increased media attention on cyberattacks and data breaches, consumers are becoming much more sophisticated, and as a result, much more demanding about what they expect from healthcare organizations from a compliance and security perspective.

Investors are more demanding as well, and from a business continuity perspective, no organization wants to be in a situation where a successful attack or breach shuts down services and steals or destroys sensitive data. The impact of such an event on revenue, cash flow, and valuation can be severe.

All of this means that healthcare technology vendors, serving as Business Associates under HIPAA, must have mature and scalable HIPAA compliance and cybersecurity capabilities.

The reality is, however, many Business Associates:

- Are unsure of requirements
- Lack necessary expertise
- Have security gaps (products built for healthcare may not necessarily have all the security controls in place, especially ones in cloud environments)
- Don’t have adequate funding or resources
- Are missing tools to manage cyber risk and compliance effectively
- Struggle with accurately responding to security questionnaires

So how do you establish a reasonable and appropriate HIPAA compliance and cybersecurity program—one that meets regulatory requirements, exceeds customer and investor expectations—and does so in a way that is cost-effective and doesn’t disrupt your operations?

It begins with understanding compliance requirements and corporate strategy and building a cybersecurity and HIPAA compliance roadmap that will meet the objectives and facilitate strategy.

Meeting expectations

Your organization should view cybersecurity and HIPAA compliance as enablers of new business and resiliency, not factors that slow you down. The challenge here is overcoming barriers, especially those related to understanding what your organization must do to achieve success.

What's a business associate?

A business associate (BA) is any person or entity that performs functions or activities involving the use or disclosure of PHI on behalf of—or providing services to—a covered entity such as healthcare providers, health plans, healthcare clearing houses, etc.

As a BA, you must enter into a Business Associate Agreement that outlines terms requiring compliance with the HIPAA Security Rule, and depending on the nature of the service you're providing, there may be HIPAA Privacy Rule and Breach Notification Rule requirements as well. You are expected to report breach information, but to whom and what those reports entail depends on the nature of the breach. Sometimes that's notifying the Office for Civil Rights (OCR), or the press, effected individuals, or other oversight and regulatory bodies.

Establishing a foundation to help your organization successfully meet all of your expectations should include setting and reviewing long-term goals and objectives, with a solid understanding of what you want and need to achieve from your compliance and security programs.

This success will be rooted in well thought-out programs supported by executive leadership and organizational-wide education, coordination, and buy-in.

10 key areas for a HIPAA compliance program

From a HIPAA compliance perspective, one way to evaluate if you're meeting expectations when it comes to protecting information is to also think broadly about cybersecurity for health information systems and then move into your HIPAA requirements, and over time, build on those controls and requirements for program maturity.

Here's a good starting point and quick overview of 10 key HIPAA compliance areas to help drive your planning and implementation:

1. Establish a privacy and security risk management and governance program
2. Develop and implement HIPAA privacy, security, and breach notification policies and procedures
3. Train all members of your workforce
4. Perform HIPAA security risk analysis

5. Build HIPAA security risk management
6. Complete HIPAA security evaluation (e.g. “compliance assessment”)
7. Complete technical testing of your environment
8. Implement a strong, proactive Business Associate management program
9. Complete Privacy Rule and Breach Rule compliance assessments
10. Document and act upon a remediation plan

When looking at these key components, you should also consider these questions:

- What safeguards should we put into place?
- How do we build an appropriate security program?
- What’s the role of executive leadership and key stakeholders for program success?

Developing a cohesive compliance and security approach

Many organizations approach HIPAA compliance and cybersecurity separately, and for a lot of reasons that makes sense. Compliance with HIPAA regulations doesn’t equal security and developing security controls doesn’t mean you’ll be fully compliant for your specific mandates. However, if you work toward building a cohesive compliance and security approach for your organization, you may quickly find, with the proper tools, that it gives you comprehensive insight into your controls, policies, and procedures. Successfully developing strategies for one area likely overlaps and meets requirements for the other.

By first understanding the goals and objectives of both your security and compliance programs, you can then evaluate which controls, policies, and procedures you need to put in place to create reasonable and appropriate programs that align with your organization’s broader strategic goals and objectives.

Next, focus on building that program. This is a key place where establishing a great relationship with your executive team is paramount and where you’ll find having executive buy-in, for example, an executive sponsor, can help you achieve greater program success, and help you tackle that first key HIPAA area: to establish your program with effective governance and oversight.

Establishing compliance program leadership

When most organizations think about what they need to successfully build a cybersecurity and HIPAA compliance program, they tend to look for a professional with security leadership and technical skills, like a Chief Information Security Officer (CISO), to drive program development and maturity. That's a solid approach, whether you hire a CISO or contract with a virtual CISO who helps many organizations simultaneously with their IT and security needs.

We're seeing with increased frequency organizations hire these professionals from outside of the healthcare industry. They may have a good understanding of technical security controls and some insight into security practices your organization should engage in, but they don't always have experience building strategic programs that meet the requirements of the healthcare industry and align with your business priorities.

Why is this important?

Because meeting healthcare requirements and building a compliance and security program that aligns with your organization's strategic goals and objectives, helps you speak a language your executives and key stakeholders understand. This communication is critical to getting the resources and support you need to build your program and mature it over time. So when you're looking for a CISO or similar professional to help you with your program, look for someone who can help you translate other goals into your cybersecurity and HIPAA compliance program.

And while your CISO can be the center point of your program development and oversight, don't forget about the role of your executive leaders and key stakeholders for governance and support. You'll want your CISO to serve in a strategic role, one that routinely interacts with your leadership team. Having a full-time CISO on board will typically cost an organization in the range of $200,000-$250,000 in salary and benefits annually.

Governance

Once you've established a program leader and are working on establishing critical relationships with your key stakeholders, you'll want to involve them in helping you develop and oversee the policies and procedures that meet your organization's cyber risk management needs.

In addition to focusing on your communication with these executives, you'll want to ensure that you've established an easy-to-understand structure, one that outlines what you need (roles and responsibilities) to lead and oversee the program.

Here are some questions to consider:

- Do you have an executive sponsor?
- Does your executive sponsor have a general understanding of your important, high-level security and compliance lexicon and requirements?
- Can your executive sponsor effectively communicate your program information to the rest of the team and board?
- Is your executive sponsor in a position that will facilitate organizational-wide buy-in and explain how each team member plays an important role in the program?
- Do you have mechanisms in place where you're routinely communicating with your executive sponsor, executive teams, and key stakeholders?
- Does your executive sponsor have mechanisms in place to further facilitate this communication throughout your organization?
- What roles will your executives and key stakeholders have in developing and overseeing policy structure?

HIPAA compliance requirements

As a healthcare organization, you're required to do a non-technical evaluation of your HIPAA Security Rule compliance, and on top of that, compliance with Privacy and Breach Notification Rules is a best practice.

But what do we mean when we talk about "non-technical evaluations?" A non-technical evaluation is looking, for example, at your compliance with the HIPAA Security Rule similar to a gap assessment where you're trying to determine if your organization meets your requirements. Sometimes, this is on a granular level. For example, do you have policies and procedures in place to meet a specific requirement and are those policies and procedures effective?

Risk management

Another important part of compliance and security program success is directly related to your risk analysis and risk management practices.

Risk management is one of the most important parts of a strong security program. So what might that look like for your organization? It begins with framing your risk management program, which entails outlining how you want to employ risk management for your organization, as well as how you will measure risks, including your organization's risk appetite.

Your risk management process isn't exactly a circular process, but it's interrelated where decisions guided by your risk management framework continuously affect your assessment, response, and monitoring strategies and processes.

Here are a few questions to consider when establishing your risk management framework:

- What's an acceptable amount of risk for your organization?
- How do you identify actual risks to your organization?
- How do you evaluate if those risks exceed your organization's risk threshold?
- How do you make treatment decisions?
- How do you mitigate risk?
- What do you do when you determine a risk exceeds your threshold?

Your risk management activities will play an important part in establishing your security controls and that, in turn, can affect your compliance status.

Security engineering and application security

Whether you have internal teams of developers creating IT solutions for you, or you're working with Business Associates to create and deliver these solutions—think SaaS services or cloud providers—you'll want to have confidence that security and compliance is engineered into the core of these new apps and services.

It's important to ensure your DevsOps team continuously assesses new or updated apps for compliance and security issues throughout the software development lifecycle (SDLC), not just at and after deployment. This can help you build confidence—and demonstrate to your customers and key stakeholders—that everyone you work with takes data security, privacy, and compliance seriously, and you're committed to staying one step ahead of attackers to reduce cyber risks and protect sensitive information.

Technical testing

Under the HIPAA Security Rule, you also should employ practices for technical evaluations of your controls, which can also be referred to as technical testing.

Not only should your DevOps team be looking at security throughout SDLC, but both your security and DevOps teams should develop a culture that supports and encourages routine technical testing to ensure you have controls in place to protect your PHI and PII, and that you're routinely checking for vulnerabilities and other security issues, so you can make plans to remediate gaps before a disruptive event.

There are a number of ways you can test your controls and practices, but three of the most common include:

- Vulnerability scanning
- Internal and external penetration testing
- Social engineering, such as simulating a phishing scheme to access credentials or other important data

For example, you may want to test your code to look for known flaws or common coding mistakes or look for common issues, like those outlined in the OWASP Top 10, especially for web apps, which are a common source of data breaches today.

When you're establishing your testing plans and procedures, it's also a good idea to remember to integrate your risk management and risk analysis measures with your technical tests. This can help you periodically validate your controls work and close gaps, not just for HIPAA requirements, but also to ensure security and reduce risk.

Emergency operations and incident management

Understanding what your organization can expect if you have a breach can significantly impact your response and recovery times. In some cases it can be as significant as moving from an event that could potentially cripple you for weeks to one that inconveniences you for a few hours.

The startling reality is many breaches go undetected for an organization for a long time, and the longer bad actors have within your systems, the more damage they can cause. Although it can take up to a year to even uncover the breach, the time associated with recovery and related issues often impact organizations for years to come, whether that's in the form of an ongoing investigations, related lawsuits, brand and reputational repair, rebuilding customer confidence, or dealing with fines and penalties that can easy reach into millions of dollars.

By planning out your emergency operation practices and developing incident management plans before a breach—which is becoming increasingly not a matter of if one may happen for organizations, but when—you can help mitigate breach impact.

Here are some questions to consider:

- Do you have an effective and efficient business continuity program?
- Do you review those plans for gaps and routinely update them?
- Do you have a disaster recovery plan?
- Are you routinely testing your plans for effectiveness? For example, have you recently conducted a tabletop exercise to see if your breach policies and procedures work as you intend them to, and if not, have you made adjustments so your real-world response is more effective? Does everyone on your team understand the importance of these plans and their individual roles and responsibilities, as well as how it contributes to organizational resiliency?

Event and incident preparation can help ensure you are prepared, and it gives you the opportunity to minimize the impact of incidents and breaches on your organization. Be sure your plans cover five critical areas: preparation, identification, containment, eradication, and recovery.

What you can do now

The reality is most organizations just don't have the time or resources for this approach. That's because, if you take a traditional approach of hiring more staff and deploying lots of disparate compliance and security solutions across your enterprise, your costs can quickly reach hundreds of thousands of dollars.

But there is a better way to solve these challenges and you can get started today—while delivering the innovative digital health solutions your customers require—easier and for far less expense than you might think.

Here are a few recommendations to set you off on your journey to build and mature an effective compliance and security program:

1. Define the vision for cybersecurity and HIPAA compliance.
2. Determine where you already have key gaps or inefficiencies and what you need to accomplish (including tools, resources, and people) to remedy these issues. Do you have the resources internally or do you have the risk appetite to build those resources to close your gaps and achieve that vision?
3. Secure an executive sponsor and begin building a relationship with that sponsor that facilitates an ongoing exchange about critical program elements, including your current success, where you have gaps, and which additional resources can help make your program stronger.
4. Make plans to ensure you're routinely communicating with your leadership team and key stakeholders about your compliance and cybersecurity metrics and effectiveness.
5. Establish roles and responsibilities that clearly define executive and key stakeholder involvement in governing your programs, including oversight and development of policies and procedures.
6. Use real-world examples, including results from your own technical tests, to demonstrate and quantify what could happen to your organization if you do not build mature compliance and security strategies and practices. For example, what would a ransomware attack or successful phishing scheme look like if threat actors successfully exploited a weakness within your enterprise? What would it cost financially? How long could the impact last? What systems could be affected?
7. Consider working with a compliance and security expert to help you on your journey. Clearwater, for example, has a free risk analysis self-review tool you can use to see where you are today on your HIPAA compliance and cybersecurity journey so you have a better understanding of the steps you need to take to get your organization where it needs to be.

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