Clearwater

Whitepaper

Connecting the Dots Between Cyber Risk and Patient Safety

How rapid tech adoption in healthcare, coupled with an evolving and expanding threat landscape, can affect quality and accessibility for patient care

Table of Contents

Introduction

As technologies for healthcare continue to evolve and adoption accelerates, institutional cybersecurity is no longer just about keeping sensitive data private and safe. Healthcare organizations no longer just face pressures from cybersecurity, compliance and regulatory mandates—or the financial or legal fallout from what could happen if you fail to meet those requirements. Ineffective cybersecurity could lead to something far more detrimental than a data breach. It could be a matter of life or death for your patients.

That's because days of air-gapping technologies from the outside world or just building secure perimeters to wall off your servers and networks from ne'er-do-wells are no longer enough. With wearable health IoT devices and other medical technologies now in and outside of the clinical setting, a single breach can put lives at risk.

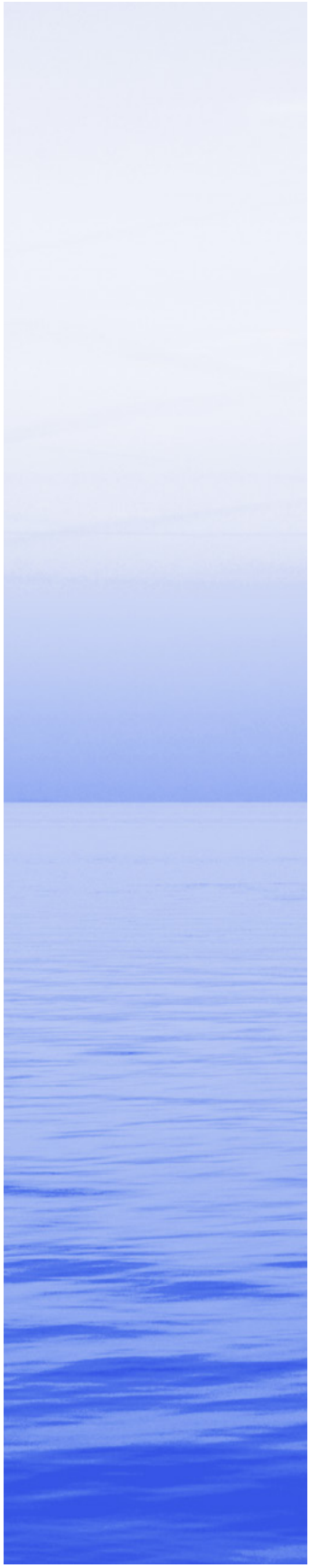
But unfortunately, many healthcare organizations struggle to connect the dots between their cyber risks and what they mean for patient safety.

It's a problem compounded by the diversity and volume of assets that can now access sensitive data such as intelligent medical devices (think smart pumps, implants, monitors and others), medical images (for example, scan results and X-rays), as well as electronic health records, patient portals, mobile health apps, laptops, smartphones, tablets, and more.

And each device/technology carries with it an expansive array of vulnerabilities and security weaknesses, all of which can be difficult to discover and mitigate or remediate before a breach occurs.

On top of that, even organizations with mature cybersecurity and risk management processes, and effective and continuous training and education are prone to human error—the one miss-click of a malicious link or inadvertent releasing of credentials that can open a door for lateral, undetected movements across your network and devices.

Today, these risks are no longer just limited to administrative headaches. They can have devastating effects on your organization's ability to operate and could ultimately negatively affect patient care and safety, possibly even resulting in loss of life.



Lawsuits, liabilities, and patient loss

Springhill Medical Center, an Alabama-based hospital, faces a lawsuit after a mother claims her child was born with a severe brain injury—and later died—because of the effects of a ransomware attack.

According to the lawsuit, the mother says she didn't know the hospital was working through a ransomware attack, which she claims affected the care of her baby during delivery.

What happened?

On July 9, 2019, Springhill Medical Center released a statement to a local news station indicating it was addressing a "security incident" that affected its internal network. That issue, according to news reports, led the medical facility to shut down its network in an attempt to mitigate the event's impact.

Ultimately, the medical center was a victim of a ransomware attack, which affected the hospital's access to its computer system because of encryption.

According to the lawsuit, the mother arrived at the hospital days later, on July 16. She claims she was not told about the issue affecting the hospital's computer systems.

The lawsuit claims that because the hospital's computers were down, healthcare providers had to use paper charts and documents throughout labor and delivery. After the child was delivered on July 17, it was determined the child suffered from brain injuries, when, according to the lawsuit, all health visits prior to delivery had appeared normal.

The lawsuit indicates that if the mother had been aware of the effects of the ransomware attack on the hospital's networks and computer systems, she would have chosen a different facility for labor and delivery, saying what happened caused permanent injuries to the child who later died on April 16, 2020, including issues related to the hospital's failure to use a fetal scalp monitor and tracing during labor and delivery.

The mother initially filed suit against the hospital in January 2020 and later amended claims after the baby died in April.

While this case is ongoing and highlights just how damaging a breach can be, in recent years there have been a number of other settlements related to healthcare data breaches, including a $500,000 settlement with the Diamond Institute for Infertility and Menopause resulting from a 2017 data breach that affected nearly 15,000 patients.

Increased ransomware attacks

While the Alabama case highlights what could go wrong in the worst way, it's unfortunately not an unlikely possibility for hospitals of all sizes today.

As we've seen since the COVID-19 outbreak, attackers have their sights finely tuned to healthcare organizations where successful ransomware attacks are on the rise.

Ransomware attacks are also becoming more complex and costly to respond to and recover from, not just for healthcare, but across most industries.

According to a report from Coveware, the average ransomware payment in Q2 of 2021 was nearly $140,000. In addition to increased ransom costs, the report says more than 80% of ransomware attacks that happened in that same time period also included the threat of stolen data leaks.

These attacks are also exposing unprecedented numbers of records. Among the top for 2021, a hacking/IT incident affecting Florida Healthy Kids Corporation in January potentially exposed some 3.5 million records. A breach in May 2021 for 20/20 Eye Care Network Inc. possibly exposed at least 3.25 million records. And just as recently as October 2021, a hacking/IT incident of Eskenazi Health may have put more than 1.5 million records at risk.

Surprisingly, these aren't among the largest record exposures experienced by healthcare organizations.

Two thousand and fifteen was an astonishing year with Anthem experiencing a hacking event that resulted in the exposure of nearly 80 million records, which resulted in a $115 million settlement. That same year, Premera Blue Cross had a hacking event that potentially exposed 11 million records and an Excellus Health breach that same year exposed about 10 million.

Phishing remains among the top causes for these types of breaches, as well as clicking malicious links, and opening malicious documents that enable attackers to infiltrate networks and systems, further spreading ransomware and other malware that cripples healthcare systems and alters, steals, deletes, or encrypts patient data.

Why are healthcare organizations such a prime target?

Attackers know healthcare providers and their business associates have access to highly valuable data such as PHI, but also personally identifiable information (PII) and other sensitive data, for example, credit card and other financial information. Some large healthcare organizations can maintain millions of records with sensitive information.

Once attackers get access to this sensitive data, they can sell it on the Dark Web or use it to steal identities, use insurance or other services in someone else's name, launch more targeted attacks, and/or destroy personal and professional reputations.

It's more than tech issues

Because discovery, response and recovery for cyber events often falls on the shoulders of IT professionals, it can be hard to see the far-reaching impacts of a breach beyond directly affected devices and data. That's a significant stumbling point for many healthcare organizations. It's not just about what happens to the device or data–but it's about the critical workflow and processes that can be stalled or stopped before, during, and after an incident.

That's why HIPAA requirements direct healthcare providers and business associates to measures that ensure not just the confidentiality of systems, data, and devices, but also their integrity and availability.

Unfortunately, in the throes of an attack, many healthcare organizations get bogged down in the technical details of their response and recovery tactics without thinking through the widespread impact on clinicians and others who may be unable to access accurate, current health data.

Why does this happen? Often, it's a result of a lack of insight, specifically caused by a failure to conduct a proper business impact assessment (BIA) and ongoing risk analysis and risk management activities to keep pace with rapidly changing environments and the evolving threat landscape.

In fact, according to an OCR report published in late 2020, most of the healthcare covered entities and business associates OCR reviewed during Phase Two audits were not compliant for HIPAA-mandated risk analysis and risk management processes.

The BIA benefit

A business impact assessment is an invaluable tool not just for ensuring HIPAA compliance, but also helping you see the big picture for your organization. It helps answer a range of questions from what your most critical systems, data, and processes are, to understanding the impact of the loss of those critical components will have on your organization's ability to do business—and keep patients safe.

A BIA can help you identify those critical components and prioritize them for response and recovery planning. *Need help conducting a BIA for your organization? Check out Clearwater's "Business Impact Analysis: Key to Operational Resilience" whitepaper for 10 strategies to ensure BIA success.*

Protecting the confidentiality, integrity, and availability of PHI

Confidentiality

Ensure PHI is not accessible and has not been disclosed to unauthorized users

Confidentiality breaches are among the most common for medical records breaches.

While there can be a number of negative outcomes for your organization and your patients for a confidentiality breach, it would not likely cause physical harm or result in patient death.

Integrity

Prohibiting changes or destruction of PHI in an unauthorized manner

While integrity breaches are less common than confidentiality breaches, they are inherently more dangerous and could affect patient care and potential results in serious injury or death. For example, gaining access to lab results and altering them or altering how a medical device functions.

Availability

Ensuring PHI accessibility and usability when needed by an authorized user

Unlike integrity and confidentiality breaches, availability breaches are generally more obvious when they occur and they can directly impact patient care and safety. For example, a patient's electronic medical record (EMR) is inaccessible before a procedure or a medical device stops functioning. This type of breach could result in patient death.

HIPAA-compliant risk analysis and risk management

You can then draw on your BIA for a thorough and effective risk analysis. Your risk assessment should take into account all risks associated with your critical data, systems, and other assets. It will help you better understand which anticipated threats may have the most impact on your ability to do business so you can plan to address those weaknesses before an incident occurs.

Your risk analysis can also give you a better understanding of what "risk" means for your organization. Drawing on OCR and NIST SP 800-30 guidance, we determine risk to be the likelihood a given threat will trigger an exploit or vulnerability and the resulting impact on your organization.

With HIPAA and OCR guidance, there is not a one-size-fits-all mandate for how to approach your risk assessments. Instead, you should take into consideration a range of variables for your organization, including, but not limited to the combination of threats and vulnerabilities for your organization, which, if an attacker exploits, would negatively affect your organization, taking into account three core components—the asset, the threat, and the vulnerability. A combination of all three likely indicates a potential threat. *Need help with your risk analysis and risk management processes? Check out Clearwater's whitepaper "Risky Business: How to Conduct a NIST-based Risk Assessment to Comply with HIPAA and Other Regulations."*

According to an OCR report published in late 2020, most of the healthcare covered entities and business associates OCR reviewed during Phase Two audits were not compliant for HIPAA-mandated risk analysis and risk management processes.

Connecting the dots

Successfully completing your BIA and risk analysis can set you on the right path toward building an effective and resilient business continuity plan, which is essential when you're anticipating and responding to a cyber event in real time.

But in addition to these processes, what else can you do to help ensure your organization sees—and responds—to cybersecurity issues with visibility into patient care impact? How do you connect the dots between HIPAA requirements for the confidentiality, integrity, and availability of PHI to quality and safe care, while ensuring timely access to that care?

1. It begins with a shift in organizational thinking. We can no longer approach cybersecurity, compliance, and risk management from the vantage point of "what will we do if we have a cyber event?" Instead, our focus should be more flexible and adaptive. Drawing on what we're seeing with increased attack severity, we must approach cybersecurity and patient safety from a "when" point-of-view. "What are we going to do when we experience a cyberattack?"

2. From there, it's important to have a good understanding—and inventory—of your organization's business ecosystem, particularly where PHI is involved. And that doesn't stop at your administrative office's doors. It also includes all of your facilities, as well as any and all business associates, partners, or vendors—even second and third (or beyond) tiers in your supply chain. They too have requirements and expectations when it comes to protecting and securing your patients' PHI and can directly affect patient safety.

3. Remember, it only takes one successful phishing or other attack vector compromise to put your sensitive patient data—and your patients' well-being—at risk. That can happen within your system or somewhere along the chain of interconnectivity between you and your business associates. It's not just about losing access to that data, which is a very real possibility with, for example, a ransomware attack, but also the response to any attack that might alter that data or make it incomplete or inaccessible for clinicians.

4. Earlier, we talked about the importance of conducting a BIA and routine HIPAA-compliant risk analysis with ongoing risk management processes. The takeaway from that is adaptability. It's imperative to always know what your most critical systems, data, and workflows are, and be prepared to re-evaluate as your environment (think adoption of new technologies) evolves and new vulnerabilities arise as in your threat landscape.

5. Consider adopting industry-recognized best practices for cybersecurity. While OCR offers guidance for HIPAA compliance, your organization may benefit

from adopting frameworks that help you plan for, implement, and manage your cybersecurity, risk management, and compliance programs. For example, the NIST Risk Management Framework and the NIST Cybersecurity Framework are great resources.

6. Know your vulnerabilities and your organization's risk tolerance threshold. Use tools that help you automatically identify those vulnerabilities and then adopt best practices to prioritize those weaknesses and make plans to either accept those risks, mitigate, or remediate them.

7. Break down the silos between privacy, compliance, risk management, cybersecurity, and other departments. As we shift from that "if" to "when" focus for cyber event impact, it's imperative to break down the silos that often wall-off critical components based on departments or locations, which all ultimately interact and affect cybersecurity and patient safety. Develop a culture of security and compliance to ensure all of your team members understand the impact and risks of a cyber event, how it may affect their roles and responsibilities, and what they can do to help protect patients and your organization from these risks.

8. Consider implementing a change management system to help your security teams stay one step ahead of any potential changes that may impact your organization's cybersecurity risks and as a result, patient safety.

Implementing a risk management program

While understanding your critical components and related risks is a great foundation for an effective cyber risk and related patient safety program, this is certainly not a one-and-done, checkbox annual exercise.

Instead, you can further mature your program and practices by developing and implementing a risk management program. This will help your organization remain aware of and adaptable to your changing environments and threat landscape without overlooking its impact on patient safety.

That's because your risk management program should be more than just assets and vulnerabilities. It also includes your governance processes (don't forget to get executive buy-in and sponsorship), as well as the people, processes, and other technologies across your organization. These should all come together in a digestible way to help build organizational understanding and engagement at all levels.

You may also find it beneficial to seek out tools that give you visibility into and the ability to automate and manage a range of processes such as risk assessments, data protection, identity management, authorization, compliance reporting, audit preparation, incident detection, incident response, and recovery, and more.

While OCR guidance and frameworks such as NIST are great to draw on to help build your cyber risk management program, remember, there's no one-size-fits-all approach to cybersecurity. As your organization has its own requirements and objectives, there is also diversity in your policies, processes, environment, and threat landscape.

Clearwater for cyber risk management

While shifting from the "if" to "when" approach to ensure cybersecurity preparedness that minimizes patient safety impact, it's important to expand your cyber risk management practices beyond a traditional approach. Stop thinking about it from a checklist or compliance-only focus. If you do, you may fall short of meeting HIPAA compliance and as a result increase risks for patient safety, too.

Clearwater can help. Clearwater's Cyber Risk Management team can help you adapt your program, planning, and management to the specifics of your organization's environment, ensuring you have ongoing, enterprise visibility into all of the threats to your critical systems, processes, and data, while planning for and effectively managing all of your risk acceptance, mitigation, and remediation strategies.

Clearwater's IRM|Pro® software-as-a-service solution can help you streamline your cybersecurity, compliance, and risk analysis processes to help you connect critical components behind the scenes directly to patient safety. And you can put away expansive spreadsheets and stack of binders with the assurance you can monitor your cyber risk management program at any time through the IRM dashboard, complete with a document repository to ensure you always have access to the information and documents you need for your cyber risk management programs.

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