

Why Adopting a Framework is Critical to a Robust Cybersecurity Program in Healthcare

Methods for enhancing healthcare system cybersecurity posture

Table of contents

Methods for enhancing healthcare system cybersecurity posture 0

The growing threat landscape in healthcare and why a framework is essential 2

 The increasing complexity of healthcare IT systems 2

 Why HIPAA is no longer enough 2

 The role of cybersecurity frameworks 3

Key benefits of adopting a cybersecurity framework in healthcare 3

 Enhanced risk management 3

 Streamlined compliance 4

 Incident response and recovery 4

 Building a culture of cybersecurity 4

 Improved patient trust 5

How to successfully implement a cybersecurity framework in healthcare 5

 Assessing your current security posture 5

 Define clear objectives and scope 6

 Assess your budget and resource constraints 6

 Allocate internal resources and build a strong team 7

 Develop a roadmap for implementation 7

 Continuous monitoring and improvement 7

Examples of popular cybersecurity frameworks 8

 NIST RMF 8

 HITRUST CSF 8

 ISO 27001 9

 Final thoughts: A strategic approach to cybersecurity 9

Appendix: Acronyms 10

 Legal disclaimer 11

 About Coalfire 11

 About the author 11

The growing threat landscape in healthcare and why a framework is essential

The healthcare industry has always been a prime target for cybercriminals due to the sensitive and valuable nature of its data. Information such as patient health records, billing information, intellectual property, and personally identifiable information (PII) have historically represented a goldmine for cyber attackers. Recently, however, the rise of new technologies and tools that are designed to enhance care delivery, such as telemedicine, electronic health records (EHR), medical Internet of Things (IoT) devices, and artificial intelligence (AI), has also expanded the attack surface, creating more entry points for cyber threats. As a result, healthcare organizations are facing a new era of cyber risks that demands a more strategic, comprehensive approach to cybersecurity.

The increasing complexity of healthcare IT systems

Healthcare IT systems have become increasingly complex in recent years. Providers are adopting cloud-based services, integrating EHR systems, and utilizing more connected devices, many of which were designed for convenience rather than security. Healthcare is now one of the most targeted sectors for cyberattacks, surpassing even financial institutions in terms of the volume and severity of breaches, with 2024 settings records in the number of reportable breaches. According to a report from the [Ponemon Institute](#), 88 percent of the healthcare organizations surveyed experienced at least one cyberattack in the past 12 months with, according to a CSO report, the average cost of a breach reaching [\\$4.8 million](#).

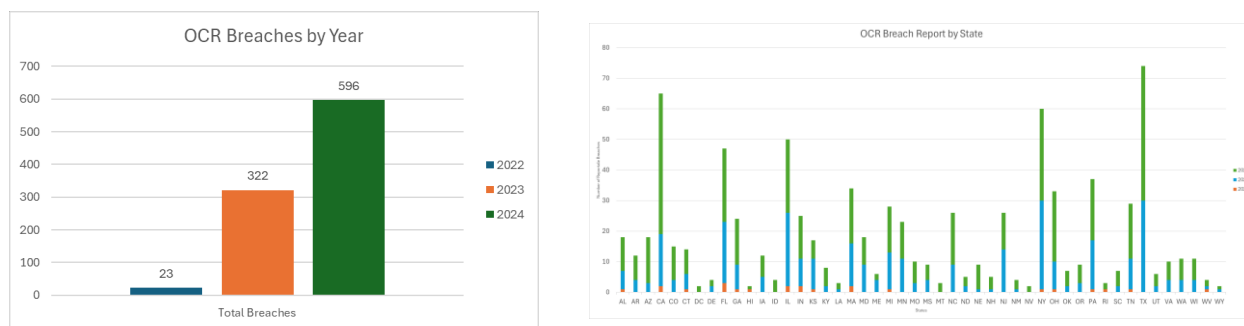


Figure 1: OCR Data Breach Totals per State and Year

The advent of technologies like AI and machine learning (ML) have also introduced new vulnerabilities. For example, AI-powered diagnostic tools require massive datasets to train models, and these datasets often include sensitive protected health information (PHI). The risk is clear: if attackers gain access to these AI systems, they can steal, manipulate, or even destroy valuable data.

Why HIPAA is no longer enough

For many years, the Health Insurance Portability and Accountability Act (HIPAA)'s Security Rule ([45 CFR Part 160 and Subparts A and C of Part 164](#)), currently being enhanced by legislation, has been the “de facto” standard for safeguarding patient data in the United States. The rule requires healthcare organizations to ensure the confidentiality, integrity, and availability of electronic PHI. However, while HIPAA compliance is still a must, it does not necessarily offer a comprehensive solution for the full spectrum of cyber threats that healthcare organizations face today.

Currently, HIPAA regulations mainly address privacy and confidentiality but do not offer detailed guidelines for tackling emerging risks such as ransomware, advanced persistent threats (APTs), or insider threats. As the threat landscape has

evolved, relying solely on HIPAA has proven inadequate for the complex and multifaceted nature of modern cyberattacks. Today, healthcare organizations need a more robust cybersecurity approach that goes beyond mere compliance and builds a solid foundation for long-term data protection.

The role of cybersecurity frameworks

This is where cybersecurity frameworks can be of use. Frameworks are structured sets of standards, best practices, and guidelines that help organizations manage and mitigate cybersecurity risks. They offer a proactive, systematic approach to security, which is essential for dealing with the rising tide of cyber threats in healthcare.

Cybersecurity frameworks like the National Institute of Standards and Technology (NIST), Health Information Trust Alliance Cybersecurity Framework (HITRUST CSF), and International Organization for Standardization (ISO) 27001, can provide healthcare organizations with clear guidelines on how to safeguard patient data, secure IT systems, and develop comprehensive risk management strategies. These frameworks offer a more dynamic approach to risk mitigation than do compliance requirements that evolves as new threats emerge.

For example, NIST offers several different frameworks (NIST 800-30, 37, 39, 53, and CSF). These options can provide healthcare organizations with an appropriate roadmap for managing cybersecurity risks across the entire life cycle, from identifying potential threats to responding to breaches and recovering from incidents.

Key benefits of adopting a cybersecurity framework in healthcare

Cybersecurity in healthcare is not just about protecting patient data; it is about ensuring that the entire healthcare ecosystem, from doctors and nurses to hospitals, insurers, and patients, remains safe and functional. The rapid adoption of digital technologies and interconnected devices has significantly expanded the scope of cybersecurity threats. As a result, healthcare organizations must go beyond a HIPAA compliance framework and implement comprehensive cybersecurity measures that offer structured, multi-layered approaches to safeguarding sensitive information. Employing such frameworks can lead to enhanced risk management, streamlined compliance, structured incident response and recovery, the building of a cybersecurity culture that can help prevent events, and improved patient trust.

Enhanced risk management

One of the primary benefits of adopting a cybersecurity framework is improved risk management. A cybersecurity framework provides organizations with a structured methodology to identify, assess, and mitigate risks. NIST 800-37 Risk Management Framework (RMF), for example, emphasizes risk management as its foundation. The framework helps organizations gain a clear understanding of their assets, systems, and vulnerabilities. By conducting risk assessments and regular vulnerability scans, healthcare organizations can prioritize their risk management efforts around the most critical threats.

This proactive risk management approach helps reduce the likelihood of cyber incidents and ensures that healthcare organizations can both prevent threat exploitation and quickly respond to emerging threats. For example, if a new ransomware variant emerges, an organization with a cybersecurity framework in place will already have processes for detecting, containing, and recovering from the attack.

Streamlined compliance

Navigating the complex regulatory environment of healthcare can be challenging given that healthcare organizations must comply with a wide range of standards and regulations, including HIPAA, California Consumer Privacy Act (CCPA), and state-specific data protection laws. A cybersecurity framework can simplify compliance by aligning its best practices with these regulatory requirements.

For instance, NIST provides a structured approach to managing cybersecurity risks while meeting compliance obligations across multiple standards, including HIPAA and NIST's own cybersecurity standards. By implementing a NIST framework, healthcare organizations can streamline their compliance efforts, ensuring they address regulatory mandates efficiently while simultaneously strengthening their security posture. The framework's comprehensive, risk-based approach offers a solid foundation for maintaining ongoing compliance and provides transparency to regulators, patients, and other stakeholders regarding the organization's commitment to safeguarding sensitive data.

Incident response and recovery

Cybersecurity breaches are inevitable, but how an organization responds can determine their ultimate cost and impact. Cybersecurity frameworks can provide healthcare organizations with structured incident response and recovery plans that enable them to react swiftly and minimize damage. The Respond and Recover functions of frameworks like NIST CSF outline the necessary steps for handling cyber incidents, including containment, communication, root cause analysis, and recovery procedures.

The having an effective incident response plan is key to mitigating the impacts of a cyberattack. In healthcare, a data breach or system outage can delay treatment, compromise patient care, and have severe financial implications. A well-developed response plan can help healthcare organizations to quickly recover from disruptions and to continue providing high-quality patient care.

Building a culture of cybersecurity

Employees represent a significant vulnerability for organizations when it comes to cyberattacks. According to IBM's [2024 Cost of a Data Breach Report](#): For the second consecutive year, phishing and stolen or compromised credentials were the most common attack vectors, accounting for 15% and 16% of breaches, respectively, and ranking among the top four costliest incident types, with compromised credential breaches averaging \$4.81 million and phishing attacks costing \$4.88 million.

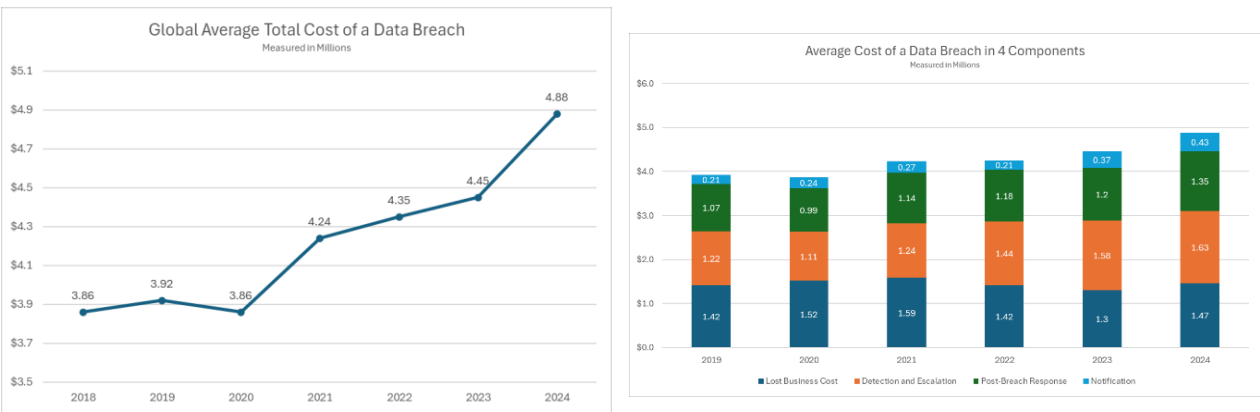


Figure 2: Cost of a Data Breach

Frameworks help mitigate these risks by promoting cybersecurity education and best practices at all levels of the organization. Adopting a cybersecurity framework can also foster a culture of security within an organization. Frameworks like NIST 800-53 and ISO 27001 emphasize the importance of employee training, awareness programs, and the continuous monitoring of internal processes. By integrating cybersecurity into daily workflows and emphasizing the importance of data protection, organizations can reduce the likelihood of security lapses caused by human error. Moreover, when leadership sets the tone for cybersecurity and allocates the necessary resources, employees are more likely to take data protection seriously and follow best practices.

Improved patient trust

Trust is the cornerstone of any healthcare organization. Patients expect their PHI and PII to be protected and handled with the utmost care, but they also expect continuity of care and access to services, even in the face of potential cyber threats. A robust cybersecurity framework helps healthcare organizations achieve both: securing patient data and ensuring that essential services remain available.

When systems like electronic medical records (EMRs) are targeted by ransomware or other cyberattacks, it can severely disrupt patient care. By implementing proven cybersecurity practices and incident response protocols, healthcare organizations demonstrate their commitment to protecting both patient data and the continuity of care. This proactive approach strengthens patient confidence, knowing that their health and their personal information are well protected, no matter what challenges may arise.

How to successfully implement a cybersecurity framework in healthcare

Adopting a cybersecurity framework is a crucial step in strengthening the security posture of healthcare organizations, but choosing the right framework is only the first step. The next challenge lies in *how* to implement it effectively. Implementing a cybersecurity framework requires thoughtful planning, adequate resources, and a clear strategy, especially considering the unique challenges healthcare organizations face, such as budget constraints, regulatory complexity, and the need for continuous adaptation in a rapidly changing digital environment.

This section walks through Coalfire's key considerations and best practices for successfully implementing a cybersecurity framework in healthcare, focusing on critical factors such as budget, organizational size, available resources, and the necessary steps to ensure long-term success.

Assessing your current security posture

Before diving into the implementation of any cybersecurity framework, the first step is to assess your organization's current security posture. This means understanding where your organization stands in terms of risk, existing controls, and potential vulnerabilities. The goal is to determine how far your current security policies, tools, and procedures align with the standards set by your chosen framework. Key considerations for assessment include:

- **Conducting a gap analysis:** Compare your current security practices against the framework's guidelines. Identify areas where your organization is already compliant and areas where improvements are needed.
- **Performing a risk assessment:** Understand the specific risks, threats, and vulnerabilities that your organization faces, from data breaches and ransomware attacks to insider threats and non-compliance with regulations like HIPAA. The U.S. Department of Health and Human Services [Office of Inspector General](#) (OIG) is placing an

emphasis on the importance of a formal compliance risk assessment being included in as part of a compliance program.

- **Involving stakeholders:** Include key departments in this assessment (e.g., IT, legal, compliance, and executive leadership) as each will have different insights into various aspects of your organization's security needs.

An accurate assessment will help you allocate resources more effectively and make informed decisions about the implementation process. Coalfire offers both security risk analysis and gap analysis services that are scalable and can be scoped to organizational needs.

Define clear objectives and scope

When implementing a cybersecurity framework, it is important to establish clear objectives and define the scope of the initiative. A well-defined plan ensures that resources are allocated effectively and that everyone in the organization understands the importance of the project. Key considerations for defining objective and scope include:

- **Setting specific goals:** Are you looking to achieve certification (e.g., HITRUST), enhance regulatory compliance (HIPAA), or simply improve overall risk management? Clearly define what success looks like for your organization.
- **Establishing scope:** Consider whether the framework will apply to your entire organization or just specific departments (e.g., IT, clinical operations, or vendor management). Some organizations start with a pilot project in a high-risk department, such as billing or patient data management, before scaling the framework across the entire organization. You also must consider, at a minimum, where your organization stores its PHI.

For example, if you are a smaller hospital with limited resources, starting small and gradually expanding may be a more manageable approach than attempting to roll out an enterprise-wide overhaul all at once.

Assess your budget and resource constraints

One of the most common barriers to implementing a cybersecurity framework in healthcare is budget. Healthcare organizations, especially smaller ones, often operate under tight financial constraints. Implementing a robust cybersecurity program can be expensive, but it is essential to view this investment as a long-term strategy to protect patient data, avoid costly data breaches, and ensure compliance with regulations. Key considerations for budgeting include:

- **Determining your budget:** Start by allocating a budget specifically for cybersecurity initiatives. Include both one-time costs (such as consulting or technology purchases) and ongoing costs (such as software subscriptions, staff training, and regular audits).
- **Prioritizing funding:** Based on your risk assessment and gap analysis, prioritize funding for the areas that will have the greatest impact. For example, if you have outdated security tools, investing in new firewalls or endpoint protection may be a priority.
- **Considering external support:** Many healthcare organizations leverage external vendors or consultants to help implement frameworks. Outsourcing certain aspects of the implementation (e.g., risk assessments, training, or technical support) can help reduce costs, especially if your in-house team lacks expertise.
- **Leveraging grants or funding:** Some government programs or industry organizations offer grants or funding opportunities to help healthcare providers improve their cybersecurity posture. Be sure to explore these options to stretch your budget further.

If resources are limited, focus on the most pressing cybersecurity issues first, such as securing patient data and ensuring compliance with HIPAA, before expanding to other areas like medical device security or supply chain risk management.

Allocate internal resources and build a strong team

Successful framework implementation requires a dedicated team, including individuals with expertise in cybersecurity, risk management, compliance, and IT. However, the size and structure of the team will vary depending on your organization's size and resources. Key considerations for internal resource allocation include:

- **Designating a cybersecurity leader:** Appoint a Chief Information Security Officer (CISO) or (a) cybersecurity manager(s) who will be responsible for driving the framework implementation. This person should have a deep understanding of both cybersecurity best practices and healthcare regulations and be identified as the official for the implementation of security policies and procedures.
- **Developing cross-department collaboration:** Involve key stakeholders from departments such as legal, IT, compliance, operations, and clinical teams. Cybersecurity in healthcare is not just an IT issue; it is an organizational-wide responsibility.
- **Ensuring proper training:** Employees across all departments need to understand their role in maintaining security. Provide regular cybersecurity training, focusing on topics like phishing prevention, password management, and data privacy. Consider utilizing resources like security operations centers (SOCs) for continuous monitoring if your budget allows.

Building a strong internal cybersecurity team can help ensure that the framework is implemented successfully and that ongoing risk management efforts are sustained.

Develop a roadmap for implementation

A detailed, step-by-step roadmap is essential for guiding the implementation process and ensuring that it stays on track. A well-structured roadmap allows you to break down complex tasks into manageable phases and set clear milestones for each stage of the implementation. Key considerations for implementation planning include:

- **Breaking it down into phases:** Rather than attempting to implement the framework all at once, divide the process into phases. For example, Phase 1 could focus on risk identification and assessment, while Phase 2 could address incident response procedures and technology upgrades.
- **Setting realistic milestones:** Create achievable goals for each phase. For example, completing a risk assessment within 30 days or implementing employee training within 90 days. These milestones should align with your overall objectives and help you measure progress.
- **Monitoring and adjusting:** Regularly review the roadmap and adjust it as needed based on changes in your organization's priorities, available resources, or evolving cybersecurity threats. Flexibility is key to successful implementation.

Ensure that each phase is properly resourced and that the necessary tools, personnel, and budget are in place before moving to the next stage.

Continuous monitoring and improvement

Cybersecurity is not a one-time project; it is an ongoing process. Even after you have successfully implemented your framework, it is important to monitor progress, identify areas for improvement, and update your security posture as new threats emerge. Key considerations for monitoring and improvement include:

- **Establishing a feedback loop:** Use regular audits and assessments to evaluate the effectiveness of your framework implementation. Are you meeting your goals? Are there any gaps or new risks that need to be addressed?
- **Conducting regular training and awareness programs:** As cybersecurity threats evolve, so should your organization's knowledge and practices. Implement periodic training to keep employees updated on new threats, policies, and best practices.
- **Adapting to new regulations and standards:** Cybersecurity is an ever-changing landscape, especially in healthcare where new regulations and guidelines frequently emerge. Ensure that your framework remains adaptable to changes in the regulatory environment.

Make cybersecurity a continuous focus within your organization. By maintaining a proactive approach and regularly reassessing your security posture, you will ensure that your healthcare organization is better equipped to handle future risks.

Examples of popular cybersecurity frameworks

Choosing the right cybersecurity framework is crucial for healthcare organizations looking to secure sensitive patient data and ensure regulatory compliance. A well-established framework can provide a structured approach to identifying risks, implementing security controls, and responding to incidents. One of the most widely recommended frameworks and a best practice for healthcare organizations is the NIST RMF. The NIST RMF offers a comprehensive and systematic approach to securing information systems, making it especially suitable for healthcare environments that must navigate complex regulatory requirements like HIPAA.

The subsections below provide further information on some of the most widely recognized frameworks used in healthcare organizations:

NIST RMF

The **NIST RMF** is a structured process designed to guide organizations in managing cybersecurity risks throughout the life cycle of an information system. It can be particularly relevant for healthcare organizations because it focuses on applying a risk-based approach to security, helping ensure that sensitive PHI is protected in alignment with regulatory requirements such as HIPAA. NIST RMF:

- Offers a comprehensive set of controls for all system types
- Is risk-based and flexible
- Is directly applicable to federal and healthcare compliance needs

HITRUST CSF

The **HITRUST CSF** is specifically tailored to the healthcare industry and integrates a wide variety of standards, including HIPAA, NIST, ISO 27001, PCI DSS, and others. HITRUST is a highly respected framework for managing and securing healthcare data and is designed to reduce complexity for organizations that need to meet multiple regulatory requirements. HITRUST CSF:

- Is specifically designed for healthcare organizations
- Facilitates HIPAA compliance and can improve overall security posture
- Provides certification that demonstrates a high level of cybersecurity maturity

ISO 27001

ISO 27001 is an internationally recognized framework for information security management. While not healthcare-specific, it provides a comprehensive approach to securing data and managing information security risks. It is widely used across industries, including healthcare, for building information security management systems (ISMSs). ISO 27001:

- Is globally recognized and suitable for multinational organizations
- Focuses on continuous improvement and risk management
- Provides a structured approach to protecting sensitive information

Final thoughts: A strategic approach to cybersecurity

Successfully implementing a cybersecurity framework in healthcare is a challenging but necessary process. By assessing your current security posture, defining clear objectives, budgeting effectively, building a dedicated team, and developing a strategic roadmap, you can implement a framework that strengthens your organization's resilience against cyber threats.

Cybersecurity is a long-term investment. One that ensures the safety and confidentiality of patient data, supports regulatory compliance, and fosters trust in your organization. Whether you are a small clinic or a large hospital system, a structured, thoughtful approach to cybersecurity will help you navigate the complexities of healthcare data protection in today's increasingly digital world. Coalfire is ready to support your organization's cybersecurity needs.

Appendix: Acronyms

Acronym	Term
AI	Artificial intelligence
APT	Advanced persistent threat
CCPA	California Consumer Privacy Act
EHR	Electronic health record
EMR	Electronic medical records
HHS	U.S. Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HITRUST CSF	Health Information Trust Alliance Cybersecurity Framework
IoT	Internet of Things
ISMS	Information security management system
ISO	International Organization for Standardization
ML	Machine learning
NIST	National Institute of Standards and Technology
OCR	Office for Civil Rights
OIG	Office of Inspector General
PHI	Protected health information
PII	Personally identifiable information
RMF	Risk management framework
SOC	Security operations center

Legal disclaimer

This white paper is provided by Coalfire Systems, Inc. or its subsidiaries (“Coalfire”) for informational purposes only. This white paper is the property of Coalfire and is protected by U.S. and international copyright laws. Unauthorized use, reproduction, or distribution of this white paper, in whole or in part, is strictly prohibited. Factual information included in this white paper has been taken from sources that Coalfire believes to be reliable, but its accuracy, completeness, or interpretation cannot be guaranteed. Information is current as of the date of this white paper only and is subject to change without notice. This white paper is provided “as-is” with no warranties, including any warranty of merchantability, fitness for a particular purpose, and non-infringement. Coalfire expressly disclaims all liability arising from or relating to the use of any information or material included in this white paper for any purpose, including any actions taken or not taken based on the contents of this white paper. You are solely responsible for making your own independent assessment of the information in this white paper and for the development, implementation, and execution of your information security program. For questions regarding any legal or compliance matters referenced in this white paper, you should consult your legal counsel, security advisor, or the relevant standard authority.

About the author

Jessica Payne, *Consultant – Healthcare Cyber Risk Services*

Jessica Payne, BS in Management Information Systems with a focus on Information Assurance, is a certified cybersecurity professional holding CompTIA Security+, CompTIA CySA+, ISC2 Certified in Cybersecurity (CC), and Certified Cyber Security Architect (CCSA) credentials. Since joining Coalfire in 2024, she has brought over five years of cybersecurity consulting experience, specializing in healthcare risk management and compliance. Jessica works closely with healthcare clients to strengthen their security postures using industry frameworks such as NIST 800-53, NIST CSF, HIPAA, and ISO 27001.

Her expertise includes conducting comprehensive security assessments, developing tailored cybersecurity programs, and ensuring regulatory compliance for healthcare organizations. Jessica has led initiatives in incident response, vulnerability management, and policy development, helping clients mitigate risks and safeguard sensitive data. Dedicated to ongoing professional growth, she stays at the forefront of cybersecurity trends to provide innovative, effective solutions that address evolving security challenges.

About Coalfire

The world's leading technology infrastructure providers, SaaS companies, and enterprises – including the top 5 cloud service providers and 8 of the top 10 SaaS businesses – rely on Coalfire to strengthen their security posture and secure their digital transformations. As the largest firm dedicated to cybersecurity, Coalfire delivers a comprehensive suite of advisory and managed services, spanning cyber strategy and risk, cloud security, threat and vulnerability management, application security, privacy, and compliance management. A proven leader in cybersecurity for the past 20 years, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success. For more information, visit [Coalfire.com](https://coalfire.com).

Copyright © 2024 Coalfire. All rights reserved. The information in this document is subject to change at any time based on revisions to applicable regulations and standards. Any forward-looking statements are not predictions and are subject to change without notice. Coalfire is not responsible for any errors or omissions.

WP_ Why Adopting a Framework is Critical to a Robust Cybersecurity Program in Healthcare_12102024