COALFIRE

DATASHEET

HIPAA security risk analysis and advisory services

Covered entities are required to comply with the risk analysis requirement mandated by the HIPAA Security Rule, MACRA, and other regulations. Similarly, business associates not only must comply with the risk analysis requirement to meet HIPAA regulations, but also need to meet customer demand in business associate agreements.

Regardless of which entity you are, the risk analysis report can demonstrate security maturity and improve your competitive position in the market. The report can also be used to show proof of due diligence in the case of a data breach or an audit by the Office for Civil Rights (OCR). Most importantly, an accurate and thorough risk analysis is foundational in determining security risks to patient information and patient safety in your environment.

The HIPAA Security Rule requires organizations that create, maintain, and transmit electronic protected health information (ePHI) to evaluate threats and vulnerabilities in their environments and implement reasonable and appropriate security measures to protect the security and integrity of ePHI. The OCR defines risk analysis "as a necessary tool to assist covered entities and business associates in conducting a comprehensive evaluation of their enterprise to identify ePHI and the risks and vulnerabilities to the ePHI." Failure to conduct an adequate risk analysis is one of the common findings in OCR audits.

The Centers for Medicare & Medicaid Services (CMS) also stresses the importance of performing security risk analysis to safeguard ePHI. CMS requires it for quality payment programs like electronic health record (EHR) meaningful use attestation in Medicare Promoting Interoperability (PI) Programs and advancing care information performance scoring in the Merit-based Incentive Payment System (MIPS).

OUR APPROACH

Coalfire's security risk analysis approach leverages the NIST 800-30 risk assessment framework and is customized based on our in-depth knowledge of threats and vulnerabilities impacting healthcare IT environments. Performing an accurate and thorough risk analysis is not possible without a deep understanding of cybersecurity threats and vulnerabilities as well as the knowledge of the healthcare environment, associated applications, and medical devices.

You can leverage our deep cybersecurity expertise, knowledge of healthcare IT, and the latest technologies to perform periodic security risk analysis to uncover risks to patient data and patient safety.

Our HIPAA security risk analysis methodology includes:

- Determination of the scope
- Data collection methodology
- Identification of potential threats and vulnerabilities
- Assessment of current security measures
- Determination of the likelihood and potential impact of threat occurrence
- Determination of your level of residual risk
- Finalized documentation
- Periodic reviews and updates to the risk assessment (based on changes that take place in the environment)

DELIVERABLES

After the HIPAA risk analysis, we deliver a summary report that identifies findings and remediation actions, which provides executive management a high-level view of potential risks in the organization. We also provide a detailed worksheet on potential threats and vulnerabilities, identified risks, implemented controls to mitigate them, and the resultant residual risk in the environment. We classify the risks as high, medium, or low, and then facilitate prioritization and risk mitigation. The worksheet can be used to create and maintain your organization's risk register.

HEALTHCARE RISK ADVISORY

If you need advice from a subject matter expert before or after the risk analysis, support in remediating identified gaps, or ongoing guidance on security risk management of patient data or medical devices, we can help. Our knowledgeable consultants offer advisory services that can help you follow best practices and properly address HIPAA risk analysis requirements.

WHY COALFIRE

- Our risk analysis experts specialize in the healthcare industry and maintain multiple security-related certifications including HITRUST, HCISPP, CISSP, and CRISC.
- We bring a deep understanding of the risks facing healthcare organizations today. Many of our risk analyses for covered entities and business associates have been reviewed and accepted during OCR audits.
- Our experience working with numerous commercial and government clients allows us to apply best practices in risk analysis to satisfy regulatory requirements. As part of our methodology, we leverage an understanding of data complexity for all clients, which delivers confidence that sensitive data is assessed in the most thorough and comprehensive manner in all environments.
- Our methodology is built on a best-practice approach to risk assessments. This approach ensures that we document known risks but also seek to uncover new risks in the given environment. Using this information, your organization can build a comprehensive and more mature security program that helps you proactively acquire adequate budget from your leadership team.
- We continuously monitor the evolving threat landscape and are an active member of the HPH Cybersecurity Group, which develops risk assessment guidance for the industry.
- Our proven expertise in standards, such as NIST, HITRUST, ISO, PCI, SOC, and other frameworks, plus knowledge of regulations that may overlap with the HIPAA Security Rule, enables us to leverage existing efforts whenever possible to reduce duplication of effort and audit fatigue.
- We are a vendor-neutral cybersecurity advisory firm that serves as a trusted advisor to executives, legal counsel, compliance managers, and security practitioners across numerous industries. We will help your organization progress from your current maturity level to your target level.

ENSURE COMPLIANCE WITH THE HIPAA SECURITY RULE.

Learn more about Coalfire's HIPAA security risk analysis and advisory services.

Coalfire.com | 877.224.8077

COALFIRE

About Coalfire

Coalfire is the cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for nearly 20 years and has offices throughout the United States and Europe. **Coalfire.com**