COALFIRE

DATASHEET

Healthcare security risk analysis, risk management, and cyber risk advisory services

Covered entities and their business associates are required to conduct an information security risk analysis and implement a corollary information security risk management plan to comply with legislation, regulations, cybersecurity framework accreditations, and payment incentive programs.

The Health Information Technology for Economic and Clinical Health Act (HITECH) and the Final Omnibus Rule strengthened the civil and criminal enforcement of HIPAA and extended the breach notification requirement to business associates. As a result, settlement actions and civil penalties related to the absence or insufficiencies of security risk analyses and risk management plans supplied to the Office for Civil Rights (OCR) have increased.

Specifically, these entities are "required" under HIPAA to comply with 45 CFR § 164.308(a)(1) "Security Management Process" standard of the HIPAA Security Rule, which stipulates the risk analysis and risk management implementation specifications.

OCR enforces the HIPAA Privacy, Breach Notification, and Security Rules and has identified a nine-step risk management process that aligns with the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF). Specifically, the recommended risk management process is adapted from NIST Special Publication (SP) 800-30, "Guide to Conducting Risk Assessments" and SP 800-39 "Managing Information Security Risk."

OCR's risk management process requires HIPAA-regulated organizations to scope their electronic protected health information (ePHI) environment to identify if specific threats can exploit potential vulnerabilities given the existence and efficacy of information security controls. This is done by analyzing the likelihood of a threat exploiting a vulnerability and the impact if the threat were realized. The likelihood and impact measurements determine an overall risk rating. If the risk is of a significant magnitude as determined by an organization's risk tolerance, it will be identified for further risk treatment or risk management.

OUR APPROACH

Coalfire's security risk analysis methodology leverages the OCR "Guidance on Risk Analysis Requirement under the HIPAA Security Rule," the NIST SP 800-30 risk assessment process, and the SP 800-39 risk management process to ensure alignment with OCR expectations for satisfying the HIPAA Security Rule standard.

To ensure we conduct an accurate and thorough risk analysis, our approach was developed by healthcare cyber risk professionals. We combine a deep understanding of the healthcare environment with a solid grasp of the threats and vulnerabilities associated with IT infrastructure, information security maturity, associated applications, and medical devices.

Our healthcare security risk analysis approach includes:

- Scoping of the environment
- Data collection and IT asset inventory review
- Identification of potential threats and vulnerabilities
- Assessment of current security measures and controls
- Determination of the likelihood of a threat occurrence, its associated impact, and the level of risk
- Completion of documentation
- Periodic reviews and updates to the risk assessment (based on changes in the environment)

DELIVERABLES

Our security risk analysis summary report identifies risks that exceed the organizational risk tolerance and includes response recommendations. We provide a technical workbook that details potential threats and vulnerabilities, identified risks, implemented controls to mitigate them, and the resultant risk rating. Risks are rated using a likelihood and impact matrix of very high, high, moderate, low, and very low. The worksheet can be leveraged to create and maintain your risk register and risk management plan.

HEALTHCARE RISK ADVISORY

If you need professional and subject matter expertise to ensure your risk management strategies and/or OCR responses align with regulatory and OCR expectations, our experts offer advisory services that can help you follow best practices and properly address the HIPAA Security Management standard and implementation specifications.

WHY COALFIRE

- Our risk analysis experts specialize in the healthcare industry and maintain multiple security-related certifications including CISSP, CRISC, HCISSP, CCFSP, and HCISPP.
- 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 methodology is built on a best-practice approach to risk assessments. We document known risks and also seek to uncover new risks in the assessed environment. Using this information, you can build a comprehensive and 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 Healthcare Sector Coordinating Council (HSCC).
- Our proven expertise in standards, such as NIST, HITRUST, ISO, PCI, SOC, and other cyber frameworks, plus knowledge of regulations that may overlap with the HIPAA Security Rule, enable us 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.

Make your compliance programs efficient and empowering with these services.

Coordinated assessments:
Simplify assessments and align efforts across frameworks to reduce audit fatigue and total cost of compliance.

Compliance management:
Maintain and improve security with year-round, proactive management of your compliance program.

Market development services:
Get return on compliance investment and grow market share with services that help you expand into new markets, create competitive differentiators, and accelerate pipeline.

HAVE CONFIDENCE IN YOUR SECURITY RISK ANALYSIS.

Discover how Coalfire combines informed cybersecurity expertise, knowledge of healthcare IT, and information security risk management best practices.

Coalfire.com | 877.224.8077

COALFIRE

About Coalfire

Coalfire is the trusted 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. For more information, visit **Coalfire.com.**

DS_HCriskanaysis_061720