COALFIRE

CASE STUDY

Major public health system improves cybersecurity risk posture with Coalfire's information risk management services

AT A GLANCE

In response to an Office for Civil Rights (OCR) inquiry, one of the nation's largest public healthcare delivery systems realized the need for an enterprise-wide HIPAA risk analysis and risk management plan. To meet OCR requirements, they partnered with Coalfire to develop a plan, close gaps, and demonstrate their commitment to HIPAA compliance, all while reducing costs.

CHALLENGE

The OCR submitted a request for the health system's most recent enterprise-wide HIPAA risk analysis and risk management plan. In addition to the request, the OCR deemed the cybersecurity risk management reports and artifacts developed by the previous assessor and submitted by the health system to be insufficient. The OCR identified that the HIPAA risk analysis and risk management plan did not meet the requirements of the HIPAA Security Rule, as specified in the Code of Federal Regulations (CFR) Risk Analysis – 45 CFR § 164.308(a)(1)(ii)(A) and Risk Management – 45 CFR § 164.308(a)(1)(ii)(B) and amplifying OCR guidance.

The OCR did not conduct a formal investigation, and the health system used the leniency as an opportunity to "right the ship" by seeking an independent, third-party assessor with experience in OCR processes and expertise in HIPAA compliance and information security risk management.

The health system engaged Coalfire to conduct a comprehensive risk analysis, assess organizational information risk tolerance, create a formal risk register, implement a formal risk management plan, conduct penetration testing, manage vendor risk, and perform a thorough HIPAA compliance assessment. While Coalfire's methodology and coordinated assessment approach provided efficiencies, the value-to-cost ratio was the most important benefit for the organization. Coalfire recommended how to structure the engagement to reduce budget impacts while providing a complete HIPAA solution. The OCR was kept in the loop from bid until contract and was instrumental in reviewing the statement of work to ensure thoroughness of approach, expertise of consultants, and appropriate methodology.

APPROACH

Coalfire employed the OCR audit protocol and used a mock-audit approach to assess against HIPAA compliance. The enterprise-wide information risk management engagement applied the OCR "Guidance on Risk Analysis Requirements under the HIPAA Security Rule;" National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, "Guide to Conducting Risk Assessments;" and NIST SP 800-39, "Managing Information Security Risk" to ensure the deliverables and final products conformed to OCR guidance and regulations.

To avoid overwhelming personnel responsible for facilities and assets, Coalfire and the health system jointly developed a three-year long strategic plan to assess the full scope of facilities and information assets that create, receive, maintain, or transmit electronic protected health information (ePHI).

During the audit, the team concurrently executed the information risk analysis, vulnerability analysis, and penetration testing. This provided a more informed risk analysis and allowed the penetration testing results to be populated into the risk register.

Coalfire concluded the first year of the engagement by submitting technical compliance and risk workbooks with recommendations, a fresh risk register, a new risk management plan, unique reporting for facilities and the enterprise, vendor risk assessments, and penetration testing results and recommendations.

RESULTS

The health system remedied several critical risks identified through risk analysis and penetration testing and improved compliance and risk processes and procedures. The engagement ensured a lock-step effort between compliance and security including a new dotted-line relationship to ensure coordination among departments. It also expanded the security team's ability to more effectively manage and control information risk to safeguard ePHI and ensure improved confidentiality, integrity, and availability of ePHI systems.

Coalfire's application of OCR-accepted risk management methodologies and compliance audit practices was instrumental in aligning the health system with OCR expectations and regulations.

Development of a risk management plan was one of the most important components of the engagement. By identify a risk threshold, the organization could ensure that risks equivalent or above the threshold were addressed as part of a risk management plan. Coalfire provided expertise regarding governance, risk response criteria, courses of action, and best practices for managing information security vulnerabilities. Now with more visibility, the organization can immediately reduce risk through mitigation and remediation.

After presenting first-year accomplishments to executive stakeholders and advising on information risk governance, the CIO concluded that Coalfire would continue to assist in solution development as a trusted advisor.

The second year began during the COVID-19 crisis, and progress continues through collaboration to adjust the schedule and coordinate activities to minimize impact to the health system.

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.**

CS_HIPAAcompliance_062920