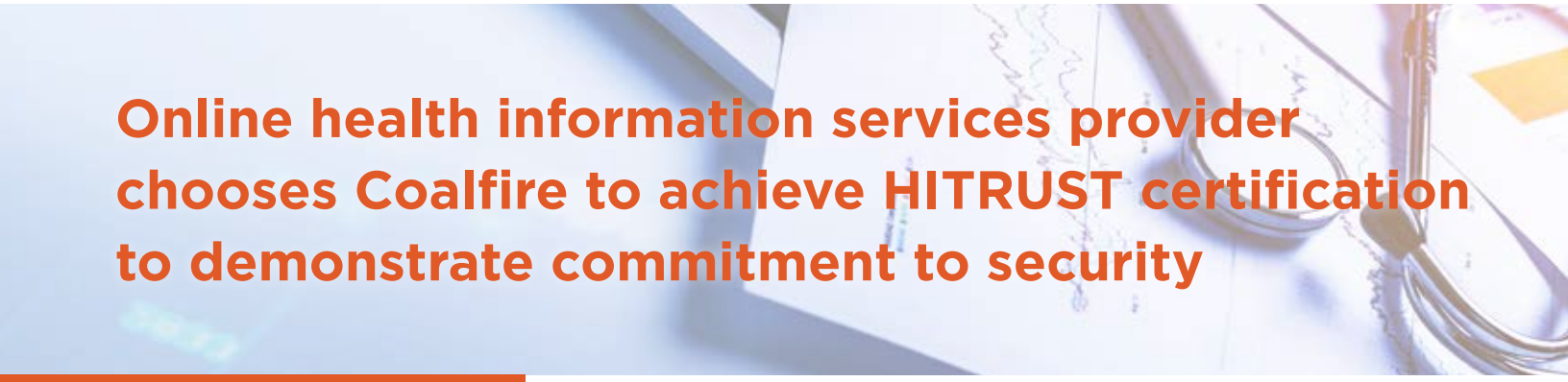
COALFIRE

CASE STUDY

Online health information services provider chooses Coalfire to achieve HITRUST certification to demonstrate commitment to security



AT A GLANCE

To better serve its growing customer base, a provider of online health information services collaborated with Coalfire to attain a HITRUST Common Security Framework (CSF) certification. As an industry leader, the company knew they needed an experienced assessor firm to successfully navigate the rigorous certification process.

"HITRUST is complex. Coalfire explained the requirements quickly and simplistically, which gave us confidence that we made the right decision to partner with them."

- CHIEF SECURITY ARCHITECT, ONLINE HEALTH SERVICES PROVIDER

CHALLENGE

According to the Protenus Breach Barometer report,[1] healthcare-related data breaches affected 5.6M patient records, representing significant organizational exposure to financial, commercial, and reputational loss. Consequently, organizations are turning to HITRUST CSF certification as an industry-recognized means of demonstrating comprehensive security compliance, risk management, and due diligence. The HITRUST CSF offers a unified approach to security, compliance, and risk that's grounded in HIPAA's security and privacy rules but also incorporates requirements from PCI DSS, the NIST Cybersecurity Framework, ISO 27001, GDPR, and other frameworks. This allows organizations to leverage the HITRUST CSF across their entire compliance and security program. The HITRUST CSF tailors composition and rigor of controls based on the organization's type, size, complexity, and regulatory status.

As an industry-recognized "seal of approval," HITRUST CSF certification can be a market differentiator and a good-faith gesture with customers.

"We chose the HITRUST CSF path to demonstrate our commitment to security to our customers," said the chief security architect at the online healthcare services provider.

The company selected Coalfire to guide them through their HITRUST CSF journey. "A former colleague used Coalfire for PCI DSS compliance, and a few partners suggested we include Coalfire in our evaluation process," said the chief security architect. "After interviewing a couple of firms, our team felt strongly about proceeding with Coalfire, largely due to Coalfire's ability to grasp our business goals and needs. Coalfire's depth of knowledge and proven experience were key in our decision."

APPROACH

The company began the HITRUST CSF journey in the fall of 2015, when Coalfire performed an initial pre-assessment of the company's HITRUST

[1] Protenus. "2017 Breach Barometer Annual Report." https://www.protenus.com/2017-breach-barometer-annual-report

CSF requirements. The pre-assessment introduced the provider to the HITRUST CSF methodology and initially characterized the company's protected health information (PHI) environment, requirements identification and assessment configuration, and readiness review of security documentation. This effort led to a larger advisory engagement in 2016 and 2017, where Coalfire provided in-depth expertise to:

- Investigate how specific HITRUST CSF requirements applied to the provider's environment.
- Determine what might be appropriate solution options to satisfy requirements.
- Define the degree to which the organization's services share security control responsibility with third-party service providers (e.g., data center vendors).

Coalfire extensively analyzed the company's security policies and procedures using a proprietary tool to capture HITRUST CSF requirements, generate scores based on security policy and process maturity, and denote specific deficiencies and remediation recommendations. The company focused primarily on policy and procedure remediation, but also engaged Coalfire to provide guidance on specific security implementation concerns regarding a few dozen of their more than 300 requirements.

The advisory work prepared them for the actual validated assessment, which began in January 2018. Coalfire dedicated a separate team to perform assessment activities (maintaining assessor/advisory separation, per HITRUST CSF requirements). The Coalfire team performed its own analysis of the company's security documentation and onsite testing of security implementations. With the benefit of the advisory phase, the organization identified and remediated many deficiencies that, during the validated assessment, would have adversely affected their chances for certification. Coalfire's team determined requirement scoring, made detailed observations, gathered supporting evidence, and then submitted these materials via the online MyCSF tool for HITRUST review and adjudication. Coalfire also facilitated HITRUST CSF questions or information requests on behalf of the company during the quality assurance (QA) phase of the HITRUST review.

The organization achieved HITRUST CSF certification in the spring of 2018 under CSF Version 8.1. From here, the company will need to complete an interim assessment by spring of 2019, as a pulse-check validation of continued compliance. Additionally, Coalfire and the company are examining options for a bridge assessment, a gap analysis of new HITRUST CSF requirements.

RESULTS

With extensive HITRUST CSF engagement experience and expert assessors, Coalfire helped the company achieve HITRUST CSF certification. "We didn't have to wait around for answers to our questions; Coalfire had answers for us almost always immediately," says the chief security architect. "Having a partner like Coalfire with its proven expertise has been a huge help along our HITRUST CSF certification journey."

As a result of certification, the company has provided peace of mind to their existing customers and attracted new business by demonstrating a commitment to ongoing security, risk management, and responsible stewardship of their customers' healthcare data.

CS_HealthSvcs_062118

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 more than 17 years and has offices throughout the United States and Europe. **Coalfire.com**