

CASE STUDY

Virtual CISO for Healthcare Compliance



Online's Security Risk Assessment and HIPAA Compliance services assisted a health technology company, based in California, meet a set of critical compliance requirements.

THE CHALLENGE

Our client needed to comply with HIPAA and potentially HITRUST, SOC2, and ISO. They had a strong technical team, including Software Engineers and Architects, however, they did not have the sufficient in-house experience to achieve and demonstrate compliance effectively, through documenting their adoption of security controls in a manner that regulators and auditors expect.

THE SOLUTION

Online's team of security experts worked with their in-house team to capture and translate existing security controls, document gaps, and oversee remediation. Our team also started the process of putting a security program in place, while ensuring that it also met the requirements of the HIPAA Security Rule.

As part of ensuring compliance with HIPAA our team used an approach with four major components:

- > Document and approve a comprehensive Information Security Policy
- > Conduct a Security Risk Assessment
- > Implement a Security Risk Management process
- > Setup a Security Team to track remediation and make risk-based decisions

Building on the earlier activities, we worked with the client to implement a robust security program that would ensure our client was positioned to meet both current and future compliance requirements. By adopting a security program, the organization could abandon operating in a reactive mode and instead be confident that they could respond effectively to questionnaires and compliance requirements when they arose.

After achieving HIPAA compliance, we also built out a security program that:

- > Fits the organization's needs without being overly burdensome
- > Implements reasonable security controls to help protect the organization against the most likely threats
- > Lays the foundation to manage and measure information security as the grow and mature.

THE RESULTS

We were able to help the organization achieve compliance with the HIPAA Security Rule in seven months and when the next vendor security assessment occurred, the team was well prepared and able to quickly address minor remediation steps required. Additionally, by performing these actions, the organization was well on its way to achieving and maintaining ISO 27001 and SOC2 Type II Certification.

NEXT STEPS

If you are a healthcare organization that is looking to avoid compliance penalties but aren't able to employ a full-time CISO, our security team can provide you with a complimentary assessment. Visit **obsglobal.com**



Contact:

Online Business Systems
1.800.668.7722
info@obsglobal.com

About Online Business Systems

Online is a digital transformation and cybersecurity consultancy. Since 1986 we have been using technology to deliver dramatic business results for companies throughout Canada, USA and EMEA. Our capabilities across the transformation cycle enable our Clients to move confidently into their secure digital future.