



Online was engaged by a large digital health company to conduct a Security Risk Assessment for HIPAA compliance. The organization provides a digital platform that is accessed by more than 45 million consumers for more than 200,000 employers and health plans.

THE CHALLENGE

As a digital health company that sells products through health plans, our client met the definition of a *Business Associate* under HIPAA, and was required to comply with the HIPAA Security Rule. To meet their compliance requirements they needed to conduct a Security Risk Assessment, but wanted this assessment completed in a way that provided value to the organization in a way that prior audits and assessments had not.

Over the year prior, our client had already been through numerous security assessments and audits including SOC2, HITRUST, PCI, and an audit by their parent company. Their request was clear: “We don’t want yet another security controls assessment.” The organization had recently enhanced its Security Risk Management program and had a real interest in understanding the risks to their ePHI and how those risks impacted the business.

THE SOLUTION

Online's approach to Security Risk Assessments aligns with NIST SP 800-30 and exceeds the requirements of the HIPAA Security Rule. By using our threat-based risk assessment approach, critical assets were identified and then analyzed by identifying realistic threats based on Online's proprietary threat database, extending the value of the assessment for our client.

Instead of simply providing a list of control gaps, our security control evaluation identified a list of threat scenarios and provided insight into how those threats could impact their business. A comprehensive report was developed which prioritized the necessary steps to reduce, mitigate, transfer, or accept the identified risks based on mandated compliance and audit requirements.

THE RESULTS

Working with Online, the digital health company met their compliance requirements, benefited from a value-driven assessment, and enabled the CISO to directly report risk to the executive committee in a way that was understood from a business requirement perspective.

Together, the company was able to action next steps, make a plan based on measurable, meaningful data, and have confidence aligning the privacy needs of their clients to industry standards, and the growth of their business.

Contact:

Online Business Systems
1.800.668.7722
info@obsglobal.com

Founded in 1986, Online Business Systems is North America's leading Digital Transformation and Cybersecurity consultancy. We help enterprise Clients by designing improved business processes enabled with secure information systems. Our unsurpassed delivery, our people, and the Online culture of loyalty, trust and commitment to mutual success set us apart.