Apgar & Associates

Healthcare Technology SME prioritizes Security Risk Analysis

A Case Study in Foresight for Growth

Case Study: Healthcare Technology SME

Apgar & Associates

"Thanks to our work with Apgar & Associates, we have confidence in our vetting process.

The unexpected result was that such a structured process would give us more options, more freedom, not less."

– Client CTO

Favorite Benefit
Revamped Vendor Partnership Policies

How it began

Boston-based Healthcare Technology SME **prioritizes Security Risk Analysis**, gains essential consulting partner Apgar & Associates, LLC to **prep for SOC 2** certification process.

A quickly growing product offering drove a Boston-based healthcare software and services company to formally review and operationalize its approach to a SOC 2 certification. Engaging Apgar & Associates to navigate the certification preparation process, the company began with the bedrock of data privacy and information security compliance activities: **the Security Risk Analysis (SRA)**.

The healthcare technology company had launched a new solution that was rapidly being adopted by healthcare covered entities across the nation. With that knowledge, and two successful product and service offerings under the company's belts, company leadership decided to demonstrably operationalize its data privacy and information security. For Apgar and Associates, that meant starting with a comprehensive Security Risk Analysis (SRA).

"We're a small team, and knew we were already punching above our weight class when we started down the path," explained the company's Chief Operations Officer. "Then came the realization that the roll-out of our newest offering was, understandably, going to take most of our resources. So, we looked for a partner that was a cultural fit plus had great references. That's how we came to work with Apgar and Associates."

Chris Apgar, CISSP, CCISO and Julia Huddleston, CIPP/US, CIPM, CCSFP have been working with covered entities and business associates for more than two decades. Their certification readiness services have helped numerous organizations successfully achieve SOC 2, HITRUST, and ISO certifications.

Huddleston spearheaded initial discussions with the healthcare IT company, and thoroughly enjoyed getting to know the team.

"It's rarer than you'd think for an entire executive team to be on board with the path to certification and willing to dedicate the time and financial resources and tolerate the potential disruption that the prep process brings with it," Huddleston shared. "**From day one, our client made it clear that they were 100% in it to win it.** They were committed to whatever was required to get to the readiness point for a successful SOC 2 attestation."

Case Study: Healthcare Technology SME

Apgar & Associates

What came next

With the rapid uptake of its new service offering, the healthcare technology SME partnered with Apgar & Associates to execute the comprehensive SRA as soon as possible.

While an SRA is typically resource-intensive, the client's Director of Client Partnerships praised Apgar & Associates for its sensitivity to the company's immediate constraints: "We didn't have a 500-person team to dedicate to the process. **Julia and Chris made the SRA and related recommendations appropriate to our organization**, and their method made the SRA far less burdensome than expected."

Huddleston quickly grasped the new client's complex product and service offerings. Together with Apgar, the two created a fully holistic assessment and analysis, taking a highly structured approach based on methods recommended by NIST and the OCR. Technical tools, administrative and operational processes, team member roles and functions – all were fair game.

The outcome

The biggest area for improvement identified by the SRA was related to how the health IT company contracted with partner vendors, so Apgar & Associates helped the client implement changes in the client's approach to vendor management. Chris Apgar, with his CCISO and EDI knowledge, weighed in heavily here, providing detailed recommendations. **The client's CTO and Apgar hammered through the nuances and complexities together.**

Because the company's newest product offering necessitated the exchange of data transfers containing substantial ePHI, the client began the process of formalizing its approach to vendor management. Knowing how its partner vendors handled infosec was imperative.

Today, the Boston-based healthcare technology company has established a vendor management program that assures it has completed full infosec review of all partners and has appropriate controls in place to monitor and review access at various intervals.

All potential vendors that may encounter the company's PHI via data exchanges must be fully vetted. At a high level, the healthcare technology company now sets out to ask several questions before sharing data with a partner:

- Will the vendor encounter potentially sensitive data, such as PHI?
- Can the potential vendor sign an approved BAA or BASA?
- Does the vendor have certifications such as SOC 2?
- Can the vendor successfully complete the client's (new) IT questionnaire?

Those answers determine whether the organization can move forward with the partnership, and under what conditions.

The guidance Apgar & Associates provided to formalize the process was invaluable. "Thanks to our work with Apgar & Associates, we have confidence in our vetting process," the company's CTO stated. "The unexpected result was that such a structured process would give us more options, more freedom, not less."

Apgar & Associates

Ready to take off on your path to certification?

Call Apgar & Associates today.

Their prep process, aka certification readiness services, have helped many organizations successfully achieve SOC 2, HITRUST, and ISO certifications.

503-384-2538
info@apgarandassoc.com

Julia Huddleston, CIPP / CIPM, CCFSP

Chris Apgar, CISSP, C|CISO