CASE STUDY

Summit Medical Group's Path to Risk Resilience

Challenge

When Rachael Britt-McGraw joined Summit Medical Group as their CIO three and a half years ago, she identified significant cybersecurity gaps. The organization needed stronger security protocols, such as password complexity and proper administrative authority, security awareness training, and someone in a dedicated security role.

The provider group was also in the process of transitioning all patient data from an older electronic health records system to a new one.

Trying to determine what initiative to prioritize was like trying to build a house while laying the foundation at the same time.

SUMMIT MEDICAL GROUP

https://www.summitmedical.com/

Provider: Summit Medical Group

Location: Knoxville, TN

Number of Locations: 92

Solution

Britt-McGraw realized that to prioritize effectively she first needed to establish a cybersecurity baseline.

"I knew we needed to start having serious conversations about cybersecurity, and having a risk assessment done was the first step in getting a clearer picture of where we stood," says Britt-McGraw.

The urgency for security progress was further highlighted after a nearby Children's Hospital experienced a breach. "We had to disconnect all our portals from the Children's Hospital network to avoid being impacted by the cyber attack," reflects Britt-McGraw. "This incident emphasized to the board the severity of the situation and clarified how vulnerable and exposed the organization was without stronger cybersecurity."

Having previously worked with Fortified Health Security, she knew they were the right team to partner with for a timely and thorough risk assessment.

Implementation

With over 90 locations, Britt-McGraw wanted to ensure that each one was thoroughly evaluated to address the whole HIPAA risk environment.

"Fortified conducts physical site assessments at multiple sites, going beyond just the technical and network vulnerabilities to look at the operational elements of our security practices, including credential checks, susceptibility to social engineering tactics, and visibility of patient information on computer screens so that we could improve our overall operations," said Britt-McGraw. "These insights were then compiled into detailed reports to help our operations team implement necessary policies, procedures, and processes."

I knew we needed to start having serious conversations about cybersecurity, and having a **risk assessment** done was the first step in getting a **clearer picture** of where we stood"

Showing versus telling is key.

The honeycomb visual has been instrumental in helping our board comprehend our gaps and vulnerabilities, as well as the progress we've made in securing our organization,"

Fortified also provided Summit with customizable templates to quickly create and document necessary policies and procedures. "These policies are essential for compliance, privacy audits, and securing favorable insurance terms," explains Britt-McGraw. "We were missing many of them, so being able to use Fortified's templates and get them created quickly was incredibly valuable."

Additionally, Fortified's risk assessment roadmap, known as "the honeycomb," proved to be a compelling communication tool for illustrating the state of their cybersecurity program. When evaluating an organization's cybersecurity program, Fortified shades in each individual cell to denote controls that have been implemented (green), existing gaps (yellow), and unaddressed vulnerabilities (red).

"Showing versus telling is key. The honeycomb visual has been instrumental in helping our board comprehend our gaps and vulnerabilities, as well as the progress we've made in securing our organization," shares Britt-McGraw. "As more of our honeycomb turns from red to green, I'm better able to secure support for additional cybersecurity resources."

The risk assessments conducted by Fortified have been **crucial to our cybersecurity maturity**, but it's their **partnership approach** that truly sets them apart.

Results

With two risk assessments completed and a third in progress, Summit Medical Group has made great strides in strengthening its cybersecurity posture, shifting from a reactive to a proactive approach.

"It's exciting and reassuring to see more yellow and green areas on our honeycomb," says Britt-McGraw. "Our risk assessment progress has helped me underscore that cybersecurity is not a one and done initiative. To successfully safeguard our organization and patients' information, we need ongoing upgrades, changes, and resources."

This shift has led to better morale within the IT team. "We have IT team members who've been here for 15 years, and now that they aren't constantly fighting fires, their confidence has significantly improved," says Britt-McGraw. "The risk assessments conducted by Fortified have been crucial to our cybersecurity maturity, but it's their partnership approach that truly sets them apart. They aren't just a vendor; they are genuinely dedicated to helping us protect our organization and patients for the long term, and that reassurance makes all the difference."