

Cybersecurity as an Operational and Clinical Risk



PONDURANCE

CASE STUDY

THE CHALLENGE

Healthcare organizations remain a primary target for cyberattacks, and the impact extends beyond downtime and data loss. A cyberattack can disrupt operations, delay access to critical services, impact clinician productivity, and erode trust.

While Gulf Coast Center's mission is delivering behavioral healthcare, its challenges are familiar to organizations across every industry: balancing security investments with operational priorities, managing limited resources, reducing risk, and building a resilient technology environment that supports the business instead of slowing it down.

STARTING THE JOURNEY

Gulf Coast Center needed a modern technology environment that aligned with its mission. Leadership worked to balance security, compliance, and modernization while allowing clinicians and staff to effectively do their jobs.

Rather than simply purchasing new security tools, the organization wanted a strategic cybersecurity partner that could provide a long-term road map, extend internal capabilities, offer 24/7 monitoring and response, and integrate seamlessly into existing workflows.

Leadership also recognized the importance of executive and board support. By treating cybersecurity as a business priority rather than solely an IT initiative, the organization was able to align investments with long-term operational goals.

OVERCOMING CHALLENGES

Maximizing Existing Technology

Modernization didn't mean purchasing more tools. It meant getting the maximum value from the technology already in place.

The team conducted a thorough assessment, consolidated tools, reduced overlap, and identified opportunities to strengthen endpoint management, identity protection, and visibility.



WATCH THE WEBINAR

Cybersecurity as an Operational and Clinical Risk



PONDURANCE

CASE STUDY

Improving Visibility

With Pondurance's help, Gulf Coast Center reduced blind spots across the environment, creating a clearer picture of assets, identities, and sensitive data.

Centralized monitoring, stronger identity controls, and actionable alerts improved the organization's ability to detect and respond to threats.

Greater visibility also gave leadership increased confidence in understanding where critical assets were located, who had access to them, and how prepared the organization was to respond to threats.

Strengthening Cyber Insurance

A detailed review of Gulf Coast Center's cyber insurance policy revealed opportunities to better align coverage with the organization's cybersecurity strategy.

Just as importantly, the process highlighted how cybersecurity and cyber insurance should work together. Understanding policy requirements, security controls, and incident response expectations helps organizations improve their overall resilience before an event occurs.

RESULTS

Today, Gulf Coast Center has greater visibility, stronger monitoring, improved alerts, enhanced incident response, and faster detection capabilities. Its cybersecurity program has evolved into an operational program that brings together people, processes, technology, governance, and strategy.

By taking a phased approach and focusing first on the highest priorities, the organization has reduced cyber risk, lowered stress on the internal team, and strengthened its ability to support day-to-day operations.

Although Gulf Coast Center's story is rooted in healthcare, the lessons extend well beyond the industry. Any organization can improve resilience by understanding its existing technology, closing visibility gaps, aligning cybersecurity with business objectives, and partnering with experts to build a security program that grows alongside the business.

SEE WHAT'S POSSIBLE WITH PONDURANCE