Clearwater

Customer Success Story | OrthoVirginia

Recovering from a cyber incident, responding to the OCR, and building a cyber resilient posture for the future

A conversation with OrthoVirginia CIO, Terri Ripley

The Problem

“It was that Swiss cheese effect; the gaps all lined up perfectly,” says Terri Ripley, CIO of OrthoVirginia, describing the perfect storm that made it possible for a cyberattacker to break into their network in the midst of the COVID-19 pandemic. While the incident itself took place in 2021, resolution with the OCR was just reached in January 2023.

Ripley, a healthcare veteran and experienced executive, says her team had been working hard to stay current on all cybersecurity requirements but struggled to get some things, like multi-factor authentication, in place. After two attempts, issues with the technology created workflow barriers, so they paused the initiative. “Honestly, we thought we were too small to be a target,” said Ripley.

And then COVID hit. OrthoVirginia sent all their non-clinical personnel home to keep them safe, protect their patients, and protect their doctors so they could continue providing care. Ripley says they knew there were risks to this decision, but they needed to act quickly, and they chose to mitigate the spread of COVID as a first priority. In hindsight, Ripley says they simply weren’t prepared to have their workforce safely access their systems remotely.

The physician-owned network of more than 130 orthopedic specialists had just ramped surgeries back up after canceling them during the worst of the pandemic and it wasn’t long after that a phishing email made for the perfect exploit, giving a cyberattacker the opportunity to encrypt their PACS images and hold them hostage to ransomware.

Though OrthoVirginia resolved the initial crisis and made several changes to bolster its cybersecurity strategy, it received a letter from the OCR approximately eight months after the original attack in response to a patient about a delay in accessing their x-ray results. OCR issued OrthoVirginia a corrective action plan that would have cost them millions of dollars to implement.

The Solution

Ripley says she knew quickly upon the cyber incident that they needed outside help to recover and prevent something similar from happening again.

Beginning with KLAS research, Ripley reviewed top performers and selected three to request proposals. “It was really important to us that we partner with someone who really knew healthcare and that would listen to us,” Ripley said. Though OrthoVirginia initially set out to find a virtual chief information security officer (vCISO), they eventually expanded the scope to include help with their risk analysis and overall strategy.

Ripley says she selected Clearwater’s ClearAdvantage® managed services program for Clearwater’s expertise in healthcare cybersecurity and compliance, experience with OCR, and overall partnership approach. ClearAdvantage delivers organizations like OrthoVirginia cybersecurity and compliance best practices, like risk analysis and vulnerability assessments, program leadership, like a vCISO, and on-demand access to cybersecurity experts all in one cost-effective program.

About OrthoVirginia

OrthoVirginia is Virginia's largest provider of expert orthopedic and therapy care which serves the needs of its patients through a team of highly trained specialists who are committed to the independent practice of medicine. Located in Hampton Roads, Lynchburg, Northern Virginia, Richmond, and Southwest Virginia, OrthoVirginia has more than 130 physicians and over 30 office locations, orthopedic urgent cares, MRI facilities, outpatient surgery centers and physical therapy clinics. Virginia Orthopedics | OrthoVirginia: Stronger Starts Here OrthoVirginia combines science, technology, and a creative approach to deliver Virginia's premier orthopedic, physical therapy, and sports medicine care.

About Clearwater

Clearwater, together with its CynergisTek subsidiary and TECH LOCK Division, helps organizations across the healthcare ecosystem move to a more secure, compliant, and resilient state so they can successfully accomplish their missions. We do this by providing a deep pool of experts across a broad range of cybersecurity, privacy, and compliance domains, purpose-built software that enables efficient identification and management of cybersecurity and compliance risks, and a tech-enabled, 24x7x365 Security Operations Center with managed threat detection and response capabilities.

ClearwaterSecurity.com

Results

Since then, OrthoVirginia has successfully implemented multi-factor authentication, the use of digital identity badges, and added components like a Cybersecurity Program Performance Assessment, technical testing, and executive tabletop exercises to their cybersecurity strategy.

When OrthoVirginia received the corrective action plan from OCR, the Clearwater team helped them appeal it. "It was scary," Ripley explained, "but the Clearwater team had experience here, too, and helped us articulate in a very transparent way what we had in place and how we were following the requirements of the HIPAA Security Rule. As a result, the OCR agreed that the corrective action plan wasn't needed."

With a robust strategy in place and a partner to help navigate new and emerging threats, Ripley says, "I sleep better at night. We're so busy getting things done that we need someone in our corner to make sure we're keeping up, measuring how we're doing against our scorecard, and ultimately giving us the confidence that we won't have to live through that nightmare again. If something does happen, we'll know we've done everything we can to prevent it."

Ripley says that having a partner like Clearwater also means they are more aware of what's happening outside their organization. She says there's a lot of value in having a partner who can help OrthoVirginia leverage lessons learned in other organizations and prevent some of the things others have also had to learn the hard way.

What OrthoVirginia Says

> *"Make sure you partner with someone who has the right experience. For us, that means healthcare experience and OCR experience—they need to know what cyber threats could affect our organization, how to protect us from them, and the right approach to usher us through it. You can't know it all yourself; finding an expert focused on cybersecurity and compliance in healthcare to be your partner is so critical."*

Terri Ripley
CIO

Learn More

Whether you need help with risk analysis, responding to OCR, or a comprehensive approach to your cybersecurity and compliance program, we can help.