LeadingAge CAST
center for aging services technologies

Case Study:
Enhancing Compliance and Cybersecurity Strategies with BlueOrange Compliance

BLUE ORANGE COMPLIANCE

RiverSpring Living

leadingage.org/cast

Categories:

- Managing Compliance
- Cybersecurity Risks

About the Organization

Organization Name:
RiverSpring Living

Main Contributor:
David Finkelstein,
Chief Information Officer

Organization Type:
Post Acute/Long-Term Care Continuum

Organization Description:
RiverSpring Living operates a comprehensive array of senior care communities and programs, serving nearly 20,000 residents annually. Situated in Riverdale, NY, its offerings include skilled nursing, independent living, assisted living, memory care services, home health care, and managed care plans.

Project Description

RiverSpring Living sought to enhance its Health Insurance Portability and Accountability Act (HIPAA) compliance and cybersecurity strategies in the face of evolving threats. BlueOrange Compliance partnered with RiverSpring to deliver tailored solutions that addressed vulnerabilities, streamlined compliance processes, and fortified the organization's overall security posture.

System Type

BlueOrange Compliance conducted evaluations on RiverSpring's information technology (IT) infrastructure, including cloud-based systems and electronic medical records (EMRs), to identify and address risks.

Describe System Embodiment

The systems under review encompassed RiverSpring Living's network architecture, data storage solutions, and cybersecurity protocols. Penetration testing simulated real-world attack scenarios to uncover vulnerabilities.

Business Model

This initiative supported RiverSpring Living's Medicare- and Medicaid-supported operations while aligning with broader organizational goals.

Implementation Approach

BlueOrange Compliance employed a structured, multiphase approach. This included conducting HIPAA risk assessments to identify compliance gaps and vulnerabilities, performing penetration testing to evaluate the resilience of RiverSpring's IT systems, and collaborating on remediation plans tailored to mitigate risks and enhance security. Additionally, staff training programs were provided to foster awareness and reduce phishing incidents.

Failing to conduct a HIPAA risk assessment is not only a violation, it can also end up leaving health care providers unaware of both current vulnerabilities and potential breaches. "BlueOrange really understands the standards, understands the risks, and understands the long-term care health care industry very well, so it can help guide us in getting closer and closer to perfection every single year," said Finkelstein. In addition to the required HIPAA risk assessment, RiverSpring sought additional assurance that its systems were not an easy mark for cybercriminals focused on targeting health care providers.

For more information contact:
Scott Code, VP CAST
scode@LeadingAge.org
(202) 508-9466
LeadingAge.org/CAST

Understanding the increasing risk and consequences of a cyberattack, many health care organizations are implementing additional methods to evaluate the effectiveness of their security efforts.

Penetration testing is one way to identify and exploit vulnerabilities, analyzing the likelihood of success of real-world attacks against an organization's IT assets and physical security. While protecting patient information is a key facet of HIPAA compliance, and proper protection of that information includes network and security systems testing, it can be tough for many health care services organizations to test and analyze network vulnerabilities. Often, health care IT departments lack the resources or expertise to design and implement testing methods that actively analyze systems for technical vulnerabilities. For RiverSpring Living, Finkelstein and his team determined that hiring a compliance partner to perform penetration testing was the right option. "BlueOrange Compliance offered a practical approach to a big security challenge, as well as a quick and easy way to validate compliance," he said. With penetration testing, the team at RiverSpring Living was able to complete a more comprehensive evaluation of the organization's security posture. "The new penetration testing made possible by BlueOrange Compliance validated and provided additional insight into potential security risks I had already suspected," Finkelstein added. "It also included remediation support with recommendations."

Advantages to the Approach

The approach ensured a proactive focus on identifying and addressing vulnerabilities before incidents occurred. Tailored solutions, including comprehensive penetration testing to identify system vulnerabilities, the implementation of robust security controls, and the establishment of continuous monitoring protocols, were developed to align with RiverSpring Living's specific operational needs, while ongoing support fostered continuous improvement in compliance and security practices.

Outcomes

The partnership yielded significant results. RiverSpring Living reduced its risk of ransomware and phishing attacks through proactive vulnerability management, streamlined its compliance processes to improve audit readiness, and enhanced confidence in its safeguarding of sensitive data across the organization.

With BlueOrange Compliance engaged as part of a robust cybersecurity strategy, RiverSpring Living continuously looks for ways to go above and beyond in compliance. "As a partner, BlueOrange Compliance helps to make sure that we are not only meeting the letter of the HIPAA regulations, but gives us guidance and assistance to identify areas that may be meeting the regulation, but not as well as they could be," said Finkelstein. "They share sample policies and procedures, or even examples of how other organizations have done this, to help RiverSpring Living get to a higher level of compliance and build a comprehensive program." The organization continues to focus on enhancing the cybersecurity part of its overall security posture, mindful of the attention cybercriminals increasingly direct toward health care. "We try to be as defensive and in-depth as possible so that we can reduce our risk and reduce our exposure to ransomware and malware attacks and all the other things that happen," said Finkelstein.

Challenges and Pitfalls to Avoid

Organizations should prioritize cybersecurity by avoiding delays in assessments due to operational pressures, emphasizing staff training as a critical layer of defense, and choosing partners with specialized expertise in health care compliance and cybersecurity.

Lessons Learned

This project demonstrated the importance of proactive engagement with compliance and cybersecurity experts, regular assessments and testing to identify and address vulnerabilities, and continuous education to build organizational awareness and resilience.

Advice to Share with Others

David Finkelstein, CIO of RiverSpring Living, shares that collaborating with BlueOrange Compliance was transformative for the organization. He highlights the importance of investing in regular risk assessments and staff education to stay ahead of emerging threats. He also recommends prioritizing proactive measures to protect sensitive data and ensure compliance.