BLUE ORANGE COMPLIANCE
A CloudWave Company

CloudWave

RiverSpring Living Boosts Cybersecurity & Compliance

Table of Contents

Overview 3

Challenges 5

Solutions 7

Next Steps 10

Overview

The healthcare industry faces a rising threat of malicious attacks that target protected and personally identifiable information. These breaches often compromise sensitive patient data and can lead to financial losses and reputational damage.

While it is essential to ensure proper regulatory compliance, many healthcare organizations are increasingly seeking additional ways to protect their systems from risk.

About RiverSpring Living

Located in Riverdale, NY, RiverSpring Living operates a comprehensive array of care facilities and services tailored to meet the diverse needs of older adults and offers a full spectrum of care solutions. Situated on a sprawling 32-acre campus along the picturesque Hudson River, RiverSpring Living has a rich history spanning over a century and stands as one of the nation's foremost senior care organizations.

At the heart of its operations is a 600-bed skilled nursing facility that is complemented by several individual independent living buildings, assisted living accommodations and accompanying programs, post-acute short-term rehabilitation, managed long-term care, senior housing options, as well as specialized services such as elder abuse prevention and memory care.

As a large healthcare organization, RiverSpring Living is responsible for the protection, safety, and privacy of all patients, employees, and other key stakeholders.

2,000+
EMPLOYEES

$1B+
OPERATING BUDGET

100+
YEARS OF PATIENT CARE

Cybersecurity and Compliance Challenges

Like many healthcare organizations, RiverSpring Living considers HIPAA compliance an important challenge as providers are legally, as well as ethically, obligated to ensure patient privacy.

HIPAA law mandates implementation of documentation, processes, and security controls to protect privacy and security in the area of health information.

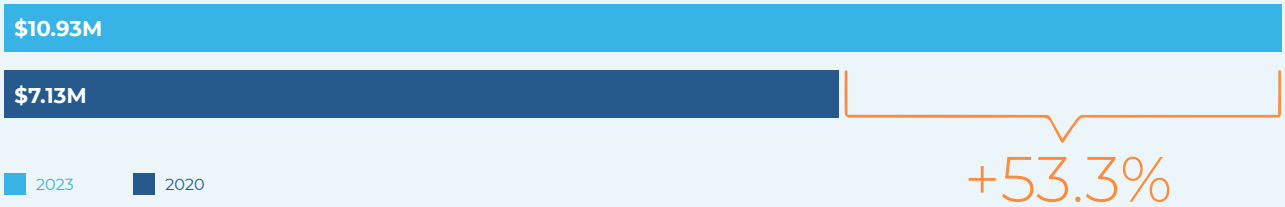
"Today, we have over two-thousand employees and serve nearly twenty thousand residents, tenants, and members," said RiverSpring Living CIO, David Finkelstein. "We are all about the resident experience and are committed to keeping records safe, while providing residents with the best life possible in whatever setting is appropriate for them."

In addition to regulatory challenges, the ongoing technology upgrades, increased vulnerabilities, and surge in cyber crime make it difficult to stay in front of emerging threats that could disrupt services.

"We are all about the resident experience and are committed to keeping records safe, while providing residents with the best life possible in whatever setting is appropriate for them."

The cost of a data breach in healthcare has increased more than fifty percent over the past three years reaching nearly **$11 million**.

SOURCE: IBM 2023 Cost of a Data Breach Report



Managing Change While Staying Compliant

The constant rate of change inherent to the modernization of IT systems and processes can also challenge teams.

"We have gone through our digital transformation journey over the past five years and moved many systems to the cloud," said Finkelstein. "In doing so, we have increased our risk."

The healthcare industry faces a rising threat of malicious attacks that target protected healthcare and personally identifiable patient information. These breaches often compromise sensitive data, leading to financial losses and reputational damage for healthcare organizations.

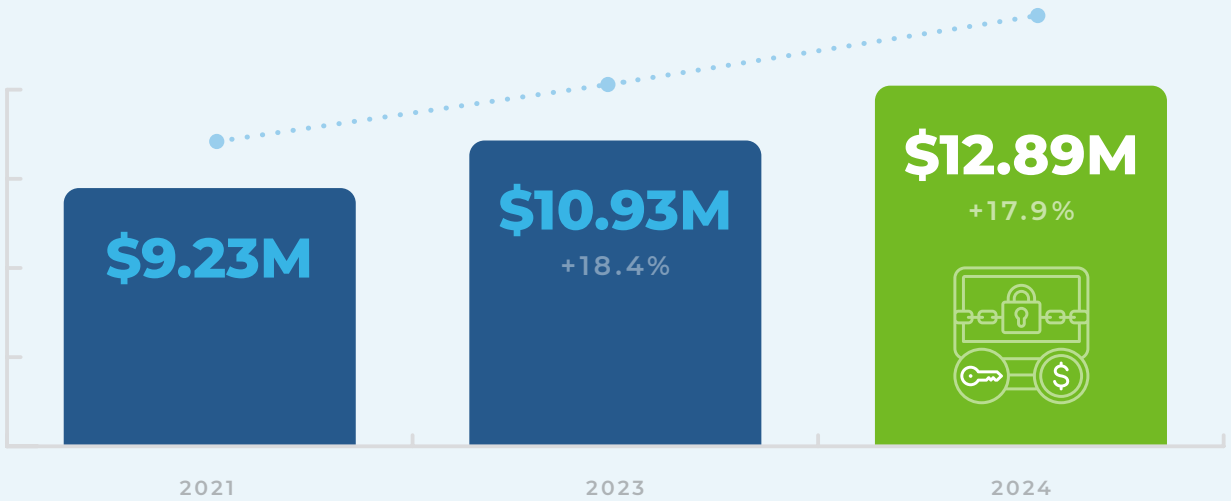
According to the IBM 2023 Cost of a Data Breach Report, the average cost of a data breach in the healthcare sector was $10.93 million. Even more concerning is this number represents a nearly 20 percent increase from the 2021 report of $9.23 million.

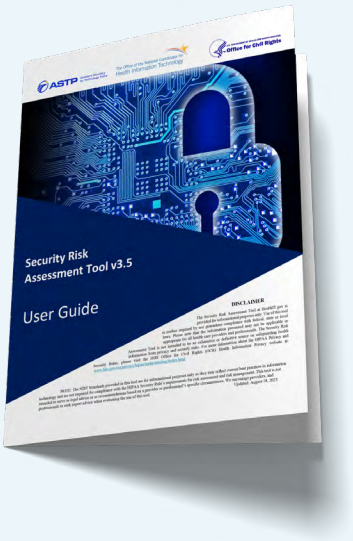
These costs include expenses related to investigation, notification, legal fees, and loss of business which will likely continue their upward climb.

"The ransomware attacks and phishing attacks are a concern," said Finkelstein. "With a workforce of 2,000+ employees, not everyone is quite as security conscious or hardened as the IT team, in order to be able to keep these things out."

While it is essential to ensure ongoing regulatory compliance, many healthcare organizations are increasingly looking for ways to protect their systems from unnecessary risk.

The Rising Cost of Cyberattacks





An Assessment of Risk

"We have used BlueOrange ever since as our vender of choice for our HIPAA risk assessment."

After initially realizing RiverSpring Living needed an ongoing cybersecurity and compliance partner, Finkelstein and his team went on the search for solutions. The first order of business was to perform the required HIPAA security risk assessment.

Mandated by the HIPAA Security Rule, a HIPAA security risk assessment is an evaluation of security policies, procedures, processes, physical security, and technology to determine whether an organization is adhering to the Security Rule requirements.

"I had found a local vendor the first year and I wasn't very happy with their knowledge of our specific niche within the healthcare marketplace," said Finkelstein. "Then I found out about BlueOrange Compliance, and we have used BlueOrange ever since as our vender of choice for our HIPAA risk assessment."

Failing to conduct such an assessment is not only a violation, it can also end up leaving healthcare providers unaware of both current vulnerabilities and potential breaches.

"BlueOrange really understands the standards, understands the risks, and understands the long-term care healthcare industry very well, so they can help guide us in getting closer and closer to perfection every single year."

In addition to the required HIPAA risk assessment, RiverSpring sought additional assurance that their systems were not an easy mark for cyber criminals focused on targeting healthcare providers.

Finding the Weakest Link

Understanding the increasing risk and consequences of a cyberattack, many healthcare 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 healthcare services organizations to test and to analyze network vulnerabilities.

Often, healthcare IT departments lack the resources or expertise that can be dedicated to the design and implementation of testing methods that actively analyze their systems for technical vulnerabilities.

In the case of RiverSpring Living, Finkelstein and his team determined that hiring a compliance partner to perform penetration testing was the right option for the organization.

"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 were able to complete a more comprehensive evaluation of their security posture.

"The new penetration testing made possible by BlueOrange Compliance validated and provided additional insight into potential security risks I had already suspected," he said. "It also included remediation support with recommendations."

"BlueOrange Compliance offered a practical approach to a big security challenge, as well as a quick and easy way to validate compliance."

David Finkelstein, RiverSpring Living CIO

Above and Beyond for Cybersecurity

With BlueOrange Compliance engaged as a part of a robust cybersecurity strategy, RiverSpring Living continuously looks for ways to go above and beyond in the area of 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 may not be as good 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 aspect of their overall security posture, mindful of the attention cyber criminals increasingly direct toward healthcare.

"We try to be as defensive and in depth as possible so that we can reduce our risk and reduce our exposure to the ransomware attacks and the malware attacks and all the other things that happen," 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."

Going Forward: Next Steps for Cybersecurity

The team at RiverSpring Living has benefited from the support of BlueOrange Compliance to provide reliable service in the area of cybersecurity and compliance and look forward to continuously streamlining their efforts.

“You don’t want surprises in this area,” Finkelstein said. “With BlueOrange, the annual risk assessment has become much more streamlined. We have the ability to use information from prior years so that we don’t have to go through things that are already fully compliant, and we just focus on areas that either have gaps from the previous year or in which there have been changes in the regulations.”

In healthcare, changes are inevitable, but a comprehensive compliance strategy with a focus on cybersecurity can help providers to protect their employees, patients, residents, and other stakeholders from unnecessary risk.

Learn more about BlueOrange Compliance and arrange to get your risk assessment or cybersecurity and compliance demo today.

Learn more →

Inspired by RiverSpring Living's success story?

Connect with us to begin your own cybersecurity and compliance journey.

BLUE ORANGE® COMPLIANCE
A CloudWave Company

855-500-6272

BlueOrangeCompliance.com

CloudWave

877-991-1991

GoCloudWave.com

ABOUT BLUEORANGE COMPLIANCE

BlueOrange Compliance, a CloudWave company, is a leader in information privacy and security, regulatory compliance, and risk management services. Together with CloudWave, BlueOrange Compliance delivers end-to-end cybersecurity solutions for healthcare organizations facing increasingly complex compliance landscapes, including HIPAA, HITECH, OCR, and other industry-specific regulations.

The combination of our proven track record in compliance audits, risk assessments, cybersecurity testing and training, and cybersecurity consulting and risk management services along with CloudWave's advanced threat detection, incident response, and cloud infrastructure capabilities results in a comprehensive set of offerings that empower healthcare organizations to secure sensitive data, streamline compliance efforts, and mitigate evolving cyber threats.

ABOUT CLOUDWAVE

CloudWave is a full-service cybersecurity and cloud services provider built exclusively for healthcare. Protecting over 350 hospitals and health system environments, CloudWave delivers end-to-end solutions that combine secure hosting, IT operations, and 24/7 threat detection and response. Services include managed security, risk and compliance, disaster recovery, systems management, and cloud optimization—all delivered with a healthcare-first mindset. Powered by AI-driven security operations and supported by U.S.-based Network and Cybersecurity Tactical Operations Centers, CloudWave provides a cyber-ready foundation for safe, uninterrupted patient care.

© 2024 BlueOrange Compliance. All rights reserved.