LeadingAge CAST
center for aging services technologies

Case Study:

Managing HIPAA Compliance and Cyber Security Through Partnership

BLUE ORANGE COMPLIANCE

WAVERLY Heights

leadingage.org/cast

Categories:

- Managing Compliance
- Assessing Risk

About the Organization

Organization Name:
Waverly Heights

Main Contributor:
Robert (Bob) Supper,
Senior Vice President and CFO

Organization Type:
Life Plan Community/Continuing Care Retirement Community

Organization Description:
For 35 years, Waverly Heights in Gladwyne, Pennsylvania, has served the senior population in Philadelphia's Main Line district. Considered a premier retirement community, Waverly Heights is situated on a 63-acre former estate with lush gardens and expansive lawns. A nationally accredited, nonprofit continuing care retirement community, Waverly Heights provides independent living, skilled nursing, personal care, and memory support services.

Project Description

Bob Supper, Senior Vice President and CFO of Waverly Heights, joined the team in 2013 with a mission to promote and enrich the organization's already strong commitment to IT security. Recognizing that complex, numerous and ever-changing compliance regulations combined with increased cyber threats can put at organization at significant risk, the Waverly team has been steadfast in ensuring continuous improvement in both security technology and cyber threat awareness.

Project Partner

Waverly Heights looked for a security partner that could help provide real-time research, analysis, and monitoring of both HIPAA compliance and cyber security. "With a previous security consulting company, we spent close to $100k to obtain a written report and boiler plate policies, with no ongoing remediation assistance," Bob recalls. "We were impressed with BlueOrange's professionalism, reasonable fees and ongoing improvement methodologies," said Bob. "In other words, our goals matched." He describes the decision to partner with BlueOrange as: "two organizations coming together with an ongoing shared commitment to IT security."

Waverly Heights and BlueOrange Compliance have been partnering together since 2015. Services provided by BlueOrange include annual HIPAA/HITECH Security Risks Assessments with ongoing managed services, HIPAA Privacy and Breach Support, Penetration Testing, and Phishing Campaigns. "We are committed to maintaining high Security and Privacy standards," Bob adds, "and we will do what it takes to protect our organization from a major breach."

Implementation Approach

BlueOrange Compliance provides the government mandated security Risk Analysis per the HIPAA Security Rule regulation CFR 164.308 (a)(ii)(A) utilizing the NIST SP 800-30, 800-53 and 800-66 risk analysis methodologies. The analysis is comprehensive, covering each Security Rule Regulation and complies to exacting government guidelines, with an approach specific to IT threats and how they relate to information security risks.

After each annual risk assessment, BlueOrange works with the Waverly team on the development and collaborative implementation of a remediation and risk mitigation plan based on assessment results.

For more information contact:
Zohra Sirat, Project Manager, CAST
zsirat@LeadingAge.org
(202) 508-9438
LeadingAge.org/CAST

Bob notes, "I like the overall process. The team is very professional with no negativity and no judgement, only understanding and support in a 'live' initiative that continues year after year." He goes on to say, that BlueOrange's secure online project management portal "has all the information we need, facilitates our back and forth communication, and helps us manage our progress and priorities."

THE SECURITY RISK ASSESSMENT EXPERIENCE

Since 2015, BlueOrange has provided Waverly Heights with an annual risk assessment designed to identify physical or process deficiencies that might allow unintended access or risk. A heavy emphasis is placed on cyber vulnerabilities and EMR use, practices, and oversight. Annual on-site visits are conducted to gather, confirm, and evaluate all pertinent security data. The entire assessment process relies on the up-to-date industry knowledge of BlueOrange Compliance staff to evaluate all relevant policies, processes, and structures, and requires a minimum amount of time from the Waverly staff.

The assessment report includes a Gap Analysis, Recommendations, and Prioritized Go Forward Plan based on the risk rating and vulnerability likelihood of each control tested. Risks are prioritized based on the severity of the impact and likelihood of an adverse event. Risk rating of maturity level percentage and corresponding stratification of 5 color coded levels of Non-Conforming (lowest) to Fully Conforms (highest) are included. These ratings are then tracked from year to year so patterns of improvement can be recorded.

"The BlueOrange Risk Analysis is like a report card to us," said Robert. "We like how it scores our performance against both the HIPAA Security Rules and NIST." Robert goes on to say, "we are a risk-conscious organization, and especially appreciate how the report ranks our risks and provides mitigation solutions."

At Waverly's request, BlueOrange CEO John DiMaggio has presented report findings to the Waverly Board and Audit committee. This collaborative approach underscores Waverly's prioritized commitment to IT security as well as the true partnership that has developed over the years between BlueOrange and Waverly. "Every board member looks at risk," said Robert, "whether it be finance, property, human resources, or technology risk. The IT Security and Privacy aspects on the BlueOrange report summarizes key risk components that the board is very interested in."

THE ONGOING MANAGED SERVICES EXPERIENCE

Since 2015, BlueOrange has also worked with Waverly on the development and collaborative implementation of a remediation plan based on the previous years' risk assessment. "We like this process because it is in real-time," notes Bob, "BlueOrange doesn't just come in and do an annual review and leave. Instead they become part of our team to help us take the steps necessary to improve." Prioritized goals, realistic project timelines, HIPAA aligned core policies, and audit support are all included.

Knowing that healthcare providers are at risk for both OCR audits and cyber-attacks, Bob reveals, "we have heard the horror stories of non-compliance and failure to keep up with evolving technology. BlueOrange's ongoing support helps us strive to be as secure as we possibly can and ensure we are doing everything feasible to maintain HIPAA compliance and reasonable security measures."

EXPERIENCE WITH OTHER BLUEORANGE SERVICES

In today's world of HIPAA regulations, not developing a plan for Privacy compliance is risky business for Healthcare providers. Multiple government agencies are actively enforcing these laws, and the penalty for non-compliance can be costly. Bob believes HIPAA Privacy and Breach remediation are a must for all healthcare organizations: "It is an ongoing process, and I was impressed with BlueOrange's approach. This is low-hanging fruit that no organization should ignore."

BlueOrange's penetration test uses the latest software tools designed to gather information, analyze, and exploit vulnerabilities, and attempt to crack passwords, decode encryption, and infiltrate operating systems, web applications, and wireless networks. The primary objective is to establish if and where unauthorized system access can be attained. Bob sees penetration testing as proactive defense against unknown vulnerabilities. "BlueOrange has very high levels of pen test execution standards, and their Pen Test Report is very comprehensive," said Bob. "They have great remediation solutions and these penetration tests have helped us keep current with patching and software upgrades."

In the quest for robust security controls, end-user practices can sometimes be overlooked. Employee carelessness, forgetfulness, and lack of knowledge can create a huge gap in an otherwise secure setting. Bob views phishing tests as a critical area in promoting accountability among staff. BlueOrange has conducted phishing expeditions on Waverly's behalf, and Waverly has since continued the initiative on their own: "We see it as an ongoing training exercise that educates our staff and hopefully prevents them from clicking on a questionable link."

Outcomes

According to Bob, the most significant outcome of the BlueOrange and Waverly partnership has been the implementation of an ongoing strategic risk mitigation plan. All parties understand that complex, ever-changing regulations, increased vulnerabilities, implementation of new technologies, and changes in business processes can make it difficult to maintain HIPAA compliance and stay in front of emerging threats.

"BlueOrange monitors and stays abreast of all the regulations and emerging threats for us," said Bob, "as we simply do not have the time to do so." "They have helped us evolve and remain secure, even as technologies continue to evolve." Bob concludes, "having BlueOrange as a partner is like having a preventative insurance policy. Together we have worked to continuously secure Waverly's IT technology and the data held within those systems."

Advice to Share with Others

Bob advises other healthcare organizations to not become complacent with IT security and HIPAA compliance: "Partnering with a security company can help you address both existing risks as well as newly emerging ones. To those who claim they cannot afford this valuable assistance, we would claim you simply can't afford not to do this, because the financial and public relations consequences could be catastrophic." Bob also suggests using a security partner that has a hands-on approach: "You want your security partner to share a mutual commitment to the continuous improvement or your organization." Finally, Bob advises organizations to not allow day-to-day operations to prevent or delay risk remediation: "Even as you juggle with your daily workloads, distractions, and other commitments, keep risk remediation at the forefront of your mind."