CASE STUDY

The Asbury Group Integrated Technologies
Anticipate More

Contributor:

Joe Kulnis

Sr. Director, Technology & Compliance

LeadingAge CAST
center for aging services technologies

The LeadingAge Center for Aging Services Technologies (CAST) is focused on accelerating the development, evaluation and adoption of emerging technologies that will transform the aging experience. As an international coalition of more than 400 technology companies, aging-services organizations, businesses, research universities and government representatives, CAST works under the auspices of LeadingAge, an association of 6,000 not-for-profit organizations dedicated to expanding the world of possibilities for aging.

For more information contact:

Zohra Sirat, Project Manager, CAST
zsirat@LeadingAge.org
(202) 508-9438
LeadingAge.org/CAST

BROADMEAD
A Dynamic Lifestyle Community

HIPAA Security Rule Compliance: Where Do I Start?

Categories

Avoidance of data breaches and consequent penalties, Enhanced Cybersecurity and Information Privacy, Improved Compliance, and Response to Cybersecurity Incident (breach, ransom, loss of mobile device(s), phishing, etc.).

Organization Name

Broadmead

Organization Type

Life Plan Community (Formerly known as Continuing Care Retirement Community (CCRC))

Other Partners

BlueOrange Compliance

Organization Description

The Stony Run Friends Meeting founded Broadmead as a way to serve the needs of older persons. It opened in 1979 as a private, not-for-profit, continuing care retirement community. Broadmead continues to operate under the guidance and ownership of a Quaker-guided, not-for-profit corporation.

The Quaker values – which speak to capacity for love, concern for one another, personal integrity, an appreciation for the simple things in life, and the belief that "There is that of God in everyone" – are still the cornerstone of this multi-denominational community. The name Broadmead comes from an historic Quaker site in England.

The property on which Broadmead stands was originally called Holly Hill. The Holly Hill farmhouse, believed to have been built in the mid to late 1700s, still stands. It's now a historic landmark known as Holly House. It serves as a Broadmead guest house and venue for private parties.

Project Description

To avoid paying massive fines, healthcare organizations must take a proactive and detailed approach to achieving HIPAA Security Rule compliance.

Broadmead wanted to do what it could to protect the electronic protected health information (ePHI) of its residents and comply with the HIPAA Security Rule. In doing so, they identified critical questions to help solve their challenge. First, where do we start without in-house expertise? Second, how do we leverage technology to aid in the effort? Finally, how can we afford the high cost associated with compliance?

Broadmead partnered with Asbury-IT to answer and the first and many more questions in pursuit of HIPAA Security Rule compliance.

Implementation/Response Approach

Asbury-IT understood a phased approach would work best in Broadmead's environment. Working closely with their Compliance Committee, Asbury-IT laid out an approach encompassing education, conducting Cybersecurity maturity assessments, establishing a corrective action plan, and a HIPAA Security Rule assessment.

Education was key throughout all phases of the project. Asbury-IT not only provided understanding of the different project phases, but also regarding the Security Rule itself and potential options in working toward compliance. Before any actual planning could be done, a baseline of Broadmead's Cybersecurity maturity was needed. Asbury-IT conducted a foundational assessment to establish the baseline, so all partners could see the starting point and have a benchmark for progress. With the assessment complete and understanding Broadmead's appetite for risk, a corrective action plan was assembled.

In developing a corrective action plan with Broadmead, Asbury-IT was able to answer their final two questions. The risk-based plan focused on technologies that required minimal overhead. However, because Broadmead was a very immature Cybersecurity environment when they first partnered with Asbury-IT, the cost of compliance seemed prohibitive. Rather than being a tactical one-year plan, the plan for Broadmead was a strategic multi-year plan that aligned to the compliance section of their strategic IT plan.

For the first year of a three-year plan, Broadmead was able to focus on low cost corrective actions and budget more expensive technologies for future years. Finally, in 2017, Broadmead's Cybersecurity maturity was at a level they felt confident to bring in a compliance assessor to validate the work done with Asbury-IT. Broadmead and Asbury-IT partnered with BlueOrange Compliance for the HIPAA Security Rule and risk assessment.

Although BlueOrange Compliance recommended Broadmead continue with their plan as Security Rule compliance never ends, they were able to confirm that Broadmead was successful in their Cybersecurity plan and approach.

Advantages to the Approach

- Builds upon Critical Security Controls recommendations for secure computing
- Methodical but flexible enough to be dynamic with economic times and technology changes
- Phased capital expenditure (CAPEX) and predictable operational expenditure (OPEX) spend
- Demonstrated due diligence with dynamic corrective action plan
- Progress is part of the organizational compliance plan and monitored by Compliance and Risk Management Committee

Outcomes

Avoidance of data breaches and consequent penalties, Enhanced System Security and Information Privacy, Improved Compliance, Improved Staff Education about Data Security and Privacy, Avoidance of Ransom, Protecting Lost/Leaked Data, Catching Phishing/Hacking Attempts, Improving Cybersecurity Resilience/Business continuity.

Lessons Learned

- The corrective action plan is dynamic; it will change along the way as technology, nature of threats, and the economy change
- Focus on ensuring that your foundational IT is an enabler to Cybersecurity
- Prioritize tasks by risk
- C-Suite sponsorship and support is essential to clearing hurdles

Advice to Share with Others

Planning for, phasing, implementing, monitoring and operationalizing a Cybersecurity plan to ensure readiness with the HIPAA Security Rule can overwhelm IT departments. Despite best efforts to do it all, IT teams are usually stretched thin dealing with the day-to-day tasks of operations and usually lack a trained Cybersecurity Officer. At the very least, organizations with this challenge should bring in an experienced partner to assess their maturity and recommend a Cybersecurity corrective plan of action.