CLEARWATER COMPLIANCE

HEALTHSOUTH®

About HealthSouth

HealthSouth is one of the nation's largest providers of post-acute healthcare services, offering both facility-based and home-based post-acute services in 36 states and Puerto Rico through its network of inpatient rehabilitation hospitals, home health agencies, and hospice agencies. HealthSouth can be found on the Web at www.healthsouth.com.

Facilities and Services

As of March 31, 2017, HealthSouth's network included 123 inpatient rehabilitation hospitals across 30 states (plus Puerto Rico); and 193 home health locations and 35 hospice locations across 25 states. In 2016, HealthSouth hospitals' inpatient rehabilitation hospital services included 165,305 inpatient discharges and 640,702 outpatient visits. In the same time period, HealthSouth oversaw 185,737 home health episodes and 3,337 hospice admissions.

Challenge:

HealthSouth sought to establish an accurate, comprehensive, OCR-quality risk analysis process to serve as the foundation for the organization's enterprise-wide security risk management program.

Solutions:

- Clearwater HIPAA Compliance and Cybersecurity BootCamp™ (education)
- IRMIAnalysis™ (software designed for HIPAA-compliant risk analysis, based on the NIST framework)
- Clearwater HIPAA Risk Analysis WorkShop™ (professional services)

Results:

- Comprehensive, OCR-quality risk analysis completed.
- Risk analysis aligns with the NIST framework.
- Risk analysis is granular, down to individual media and medical devices where ePHI resides.
- IRMIAnalysis™ software supports ongoing risk analysis and risk management, consistent with a constantly evolving asset, threat and vulnerability environment.
- Increased confidence in accuracy, detail, timeliness and scope of risk analysis.
- Anticipated savings in resources needed to generate Board-required risk assessment.

Customer Success Story

HealthSouth Automates HIPAA-Compliant Risk Assessment to Strengthen Security Risk Management

Clearwater Compliance provided the training, software, and professional services HealthSouth needed to establish an ongoing, computer-assisted, enterprise-wide risk assessment process.

Comprehensive risk analysis is a critical first step in cyber risk management. It's like that old adage, "The best defense is a good offense." How can you defend your organization against cyberattacks if you don't know where your assets and vulnerabilities are? The answer is: you can't. That is why risk analysis is so important.

That is also why the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and subsequent guidance from the Department of Health and Human Services (HHS) and the Office for Civil Rights (OCR) emphasize the importance of risk analysis. To comply with the HIPAA Security Rule (45 C.F.R. §§ 164.302 – 318), healthcare organizations must conduct "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."

"Clearwater's tool was the only user accessible software I found that operationalized the NIST framework through automation and made it manageable to apply across our assets. I could not find another vendor providing this type of software solution targeted at risk assessment automation."

— MITCH THOMAS, Chief Security Officer, HealthSouth

"Conducting a risk assessment is essential to establishing an effective cyber risk management program," said Mitch Thomas, chief security officer (CSO), HealthSouth. Besides serving as HealthSouth's CSO, Thomas is also a reservist in the U.S. military working within the U.S. Cyber Command. "I have had visibility into a good number of organizations across government and industry, so I am familiar with a lot of different approaches to managing risk," Thomas said. "I've found that performing a comprehensive, HIPAA-compliant risk assessment in a large healthcare organization is easier said than done."

The Challenge

HealthSouth had previously used multiple approaches to risk analysis with varying results. When Thomas came on board as CSO, HealthSouth was "challenged like most healthcare organizations in communicating risk and their controls in a construct that could be aligned with regulations and OCR audit expectations," he said. "We needed to establish risk management processes that correlated directly with OCR guidance."

One challenge HealthSouth faced was the vast scope and complexity of the organization. HealthSouth is one of the nation's largest providers of post-acute healthcare services. Facilities include 123 rehabilitation hospitals located across 30 states (plus Puerto Rico). The organization also includes 193 home health locations and 35 hospice locations spread across 25 states. That means HealthSouth is dealing with an enormous volume of information assets. Those assets are also widely distributed, both geographically (across facilities and across states) and organizationally (across different lines of business).

HealthSouth also regularly expands its footprint via strategic acquisitions. This means the scope of information assets, threats, vulnerabilities and security controls is continuously evolving. Thomas found previous attempts at risk assessment to be inadequate because they did not take into account the dynamic nature of the organization and external environment. "We needed something more than a static, once-a-year risk analysis report," Thomas said. "We needed a process that would give us the ability to continuously adjust our risk assessment as we established new business lines, acquired new devices, and made changes to software."

HealthSouth also shared a basic challenge common to all healthcare organizations as they worked to implement an OCR-compliant risk analysis. Namely, while the HIPAA legislation and OCR guidance explicitly states that organizations must conduct a risk assessment, the exact form that assessment should take is open to interpretation.

"One of the challenges in healthcare information security is to understand exactly what OCR is looking for, what constitutes a good security risk management process, and what a compliant risk assessment report should look like," said Thomas. OCR guidelines implicitly suggest that healthcare organizations adopt the National Institute of Standards and Technology (NIST) Cybersecurity Framework. That is helpful guidance, but once again begs the question: how, exactly, can a healthcare provider operationalize the NIST approach to cyber risk assessment?

The Solution

Shortly after Thomas started at HealthSouth, he had the opportunity to participate in Clearwater's HIPAA Compliance and Cybersecurity BootCamp™. Clearwater Compliance periodically offers live, in-person, educational BootCamps™. Clearwater also offers a virtual version of the BootCamp™. The BootCamp™ content and format can be tailored for specific organizations and associations.

In Thomas' case, the Association for Executives in Healthcare Information Security (AEHIS) was offering a five-week virtual BootCamp™ exclusively for AEHIS members. After the first session, Thomas knew he had found the risk assessment solution he was looking for.

"I wanted a solution that would tightly follow the NIST framework. At that first session, I saw that Clearwater's

solutions not only followed the NIST framework, but also automated the process, making it much easier for an organization like HealthSouth to manage and maintain," Thomas said. "I saw a clear alignment between OCR guidelines and what Clearwater Compliance was doing."

Clearwater Compliance's software suite, IRM|Pro™, is based on the NIST framework and HIPAA regulations. The suite's four stand-alone modules—IRM|Analysis™, IRM|Privacy™, IRM|Security™, and IRM|Framework™—address and automate different aspects of HIPAA compliance. HealthSouth was particularly interested in IRM|Analysis™, which would allow them to implement and automate an OCR-compliant risk analysis process across their vast and complex enterprise. "Clearwater's tool was the only user accessible software I found that operationalized the NIST framework through automation and made it manageable to apply across our assets," said Thomas. I could not find another vendor providing this type of software solution targeted at risk assessment automation."

Clearwater Compliance uses the software-as-a-service (SaaS) distribution model. The advantages of using a cloud-based (SaaS) model, rather than an on-premise model, are that there are no upfront capital costs and deployment can happen relatively quickly. Clearwater offers a continuum of services related to software deployment. At the most basic level, Clearwater offers a software subscription plus training on how to use the software effectively. Alternatively, organizations can purchase a subscription to the software with a block of time for additional professional services.

A third option is to purchase the software along with Clearwater's HIPAA Risk Analysis WorkShop™. In this version of the software implementation, Clearwater not only deploys the software and trains users, but also conducts the initial risk assessment. This gives the organization an opportunity to learn the NIST risk analysis methodology at the same time they are learning to use the software. HealthSouth chose the third option: a software subscription plus user training plus project management and professional services to conduct the initial risk analysis.

"It was immensely valuable to have Clearwater come in and help us collect the information we needed," said Thomas. "Clearwater interviewed staff across the company to identify and document information assets. They helped us analyze and organize those assets in a way that optimized efficient use of the process and the software. We didn't have to go through weeks of learning and training to get to that point.

"Clearwater was able to come in on day one, start the risk assessment process, and minimize the impact on my staff and others across the company. In just a couple of days, they accomplished what it would have taken us weeks to do on our own. Then they input all of that information into the software and worked with my team on how they did it, what that process was, and how to use the software. That gave us exactly the momentum we needed to manage and maintain the process going forward."

The Results

The entire process, from software deployment to completion of the risk analysis, was finished in six months. At the end of that period, HealthSouth had a complete, OCR-compliant, risk analysis report in hand, including findings, observations and recommendations.

Thomas said the implementation of Clearwater Compliance's NIST-based software and process led to additional positive outcomes beyond the completion of HealthSouth's risk assessment report, including the following benefits:

- **Centralized risk data.** All of the data documenting HealthSouth's information assets is now centralized in a single system: Clearwater's IRM|Analysis™. "Having all of our assets and their risks reflected within one system simplifies how we manage and report security risk" he said.

- **Real-time risk analysis.** HealthSouth now has tools and processes in place that enable real-time capability for managing assets and risk. The organization is no longer dependent on static, point-in-time risk assessments, which quickly become outdated.

- **The ability to adjust risk tolerance.** The dashboard and embedded reports in IRM|Analysis™ provide the security team and leadership the insight they need to adjust risk tolerance. "As we address risk items and mitigate them, we are able to adjust our risk tolerance threshold to address even lower risk items. This helps the team manage and communicate security risk with leadership across the organization," Thomas said.

- **Easy report generation.** The built-in reporting feature in IRMIAnalysis™ makes it easy to generate up-to-date risk analysis reports for any entity that requests a risk assessment, whether that is HealthSouth's executive leadership, the Board of Directors, the organization's insurance risk provider, OCR, or a third-party auditor.

- **Increased confidence in risk analysis findings.** "I have confidence now in how we are tracking our security risk from a compliance standpoint. Having current and detailed risk information all organized in one place provides me with the assurances I need that we are addressing our regulatory requirements. And I feel confident that we are also compliant with OCR guidelines," Thomas said.

Thomas expects the partnership between HealthSouth and Clearwater Compliance to continue into the foreseeable future. "It's been a very collaborative relationship," he said. "Clearwater Compliance has been very responsive to our needs and supportive in helping us achieve our risk assessment objectives."

"It's been a very collaborative relationship. Clearwater Compliance has been very responsive to our needs and supportive in helping us achieve our risk assessment objectives."

— MITCH THOMAS,
Chief Security Officer,
HealthSouth

CLEARWATER COMPLIANCE

About Clearwater Compliance

Clearwater Compliance, LLC is a leading provider of healthcare compliance and cyber risk management solutions. Its mission is to empower hospitals and health systems to successfully manage healthcare's evolving cybersecurity risks and ensure patient safety. Exclusively endorsed by the American Hospital Association, Clearwater solutions have been deployed within hundreds of hospitals and health systems, Fortune 100 organizations and federal government institutions. Clearwater's award-winning solutions have earned the trust of many of today's largest and most prestigious hospitals and health systems by consistently delivering innovative solutions that address today's evolving cyber threats. More information about Clearwater Compliance is at: **http://www.clearwatercompliance.com.**

AMERICAN HOSPITAL ASSOCIATION ™ ENDORSED BY THE

Health Care Information Privacy, Security, Compliance and Risk Management Solutions from Clearwater Compliance LLC have earned the exclusive endorsement of the American Hospital Association.

Call Us Today! 1.800.704.3394 | info@clearwatercompliance.com