Customer Success Story

Horizon Health Care, Inc.

Comprehensive Security Risk Analysis Helps FQHC Achieve Meaningful Use and Safeguard PHI.

ClearDATA
SECURE • HEALTHCARE • CLOUD

Horizon Health Care, Inc.

Comprehensive Security Risk Analysis Helps FQHC Achieve Meaningful Use and Safeguard PHI.

Table of Contents

Overview

Horizon Health Care, Inc. (Horizon), the largest Federally Qualified Health Center (FQHC) in South Dakota, provides personalized, affordable, high-quality healthcare through a rural community-based network in South Dakota. With 19 medical and four dental clinics, the organization takes every precautionary measure to rigorously safeguard protected health information (PHI). Securing PHI not only puts patients at ease, but also enables Horizon to meet government mandates such as HIPAA and Meaningful Use (MU) Stages 1, 2, and 3 to receive MU incentive funding from the federal government.

Facing increasing pressure to prevent, detect, and quickly remediate PHI-centric breaches, Horizon's Chief Information and Security Officer Scott Weatherill and his team chose ClearDATA to conduct thorough security risk assessments (SRAs) on a regular basis. Recognizing the value, 10 other FQHCs in the Dakotas such as allPOINTS Health Services, Prairie Community Health, and Coal Country have since followed suit. Engaging ClearDATA to conduct regular SRAs has become a key strategy to maintain HIPAA compliance, keep PHI secure and meet the qualifications for Meaningful Use funding.

"We are often seen as being at the forefront of integrating technologies and healthcare compliance processes in the Dakotas region," says Weatherill. "That's why nearly a dozen other FQHCs followed our lead and chose ClearDATA to begin conducting their SRAs."

The Challenge

For any healthcare organization, establishing accountability through data-use monitoring and security audits is no longer optional. Any security program is now required to have mechanisms and processes that enable them to assess compliance with policy and provide feedback on the effectiveness of PHI data controls. The consequences of non-compliance can be severe, including sizeable fines, loss of client confidence, and even the risk of going out of business. however, securing PHI is not always easy.

Until conducting SRAs with ClearDATA, Horizon did not have a clear picture of how to control and monitor use of PHI - especially if it was being accessed through mobile devices. Horizon staff was accessing the electronic health record systems (EHRs) and other sources of PHI from off-site locations using a variety of mobile technologies. The organization also was not fully aware of how to prioritize access controls and safeguards, train employees on proper processes, mitigate security breaches, and identify and notify patients of any potential or actual breaches.

The Solution

Knowing that SRAs had to become a mandatory and routine part of its operations, Horizon contacted its local Regional Extension Center (REC) in South Dakota for advice. RECs serve as support and resource centers to assist healthcare providers such as Horizon in EHR implementation and other health IT needs. Hands down, the local REC recommended ClearDATA as the superior option to begin and continue conducting SRAs for Horizon.

“When our local REC - which has close ties to our local university that specializes in information assurance and security - recommended ClearDATA, we knew ClearDATA had their ducks in a row,” says Weatherill. “We did consider a smaller local security company, but their costs were higher and they didn’t have healthcare-specific experience. On the other hand, ClearDATA was less expensive and 100% healthcare-focused, so immediately they knew our information security needs inside and out.”

The Results

ClearDATA conducted the first and then subsequent SRAs, and Horizon has made tremendous strides forward in protecting PHI. After meeting MU 1 requirements, the healthcare organization has moved on to conduct SRAs pertaining to MU 2 and soon, MU 3. Each time, ClearDATA has provided comprehensive, meaningful, and prioritized findings, accompanied with clear and actionable remediation recommendations.

ClearDATA went above and beyond by presenting comprehensive findings, professionally, in person, to executive staff so that any deficiencies could be presented in a solutions-focused manner and not seen as shortcomings.

"Protecting PHI can be a sensitive issue," says Weatherill. "ClearDATA, by presenting what needed to be done from an outside expertise perspective, helped us avoid pointing fingers or placing blame on what can be an extremely sensitive topic. That kind of high-touch experience from an outside consultancy is rare and greatly appreciated."

ClearDATA's findings were not only comprehensive, but also in some instances, surprising. "For me, the social engineering aspect was fascinating," says Weatherill. "The ClearDATA team physically went into our clinics and tried to get past the front desk or through the back door to access PHI. Their results were an eye-opener that let us know for certain: more employee training was required for us to protect sensitive PHI."

Horizon, too, had to tighten processes around employee termination or retirement, and ensure that no one left facilities with any type of PHI on any device. ClearDATA ensured that human resources immediately turned off access to systems such as the EMR to protect PHI. Additionally, ClearDATA taught Horizon how to detect suspected breaches and identify, notify, and respond to any patients who might potentially be affected to mitigate risks and maintain patient confidence.

Horizon soon discovered through the ClearDATA SRAs that the EHR information on its database server was not encrypted, and has since upgraded its server to include hard drives with native encryption. The same level of encryption, protection against loss, and ability to "wipe" devices now encompasses mobile devices, enabling workers to access information on the go, while reducing the risk of compromising PHI. Horizon also worked with ClearDATA to integrate SSL encryption into its existing virtual private network to enable anyone on any device to connect more securely to systems such as the EMR.

From a process and awareness standpoint, Horizon has since formed a security workgroup that meets weekly to review findings and update policies and procedures to ensure that encryption, policies, training, and other factors are up-to-date. The organization has become more astute and diligent about reviewing firewall logs, and, with ClearDATA's assistance, has put employees and executives through security awareness training, based on the recommendations from ClearDATA's findings.

When asked if he ever had an opportunity to advise other healthcare organizations concerned with safeguarding PHI, Weatherill says, "Invest in staff training. You can throw all sorts of technology at the issue - firewalls and encryption for example - but we found that staff awareness and behaviors were our weakest link. Employees need to be trained by experts such as ClearDATA. If employees are taping passwords to their computer monitors or are unable to identify what looks like phishing or malware, then technology is a futile investment. And first and foremost, hire ClearDATA, because they know healthcare security and privacy like no other company."

About Us

ClearDATA is the nation's fastest growing healthcare cloud computing company. More than 310,000 healthcare professionals rely on ClearDATA's HIPAA compliant cloud computing HealthDATA platform and infrastructure to store, manage, protect and share their patient data and critical applications.

ClearDATA
SECURE • HEALTHCARE • CLOUD