CUSTOMER SUCCESS STORY

St Charles Healthcare System

Healthcare

> "Within literally minutes of the appliance being plugged in, we started collecting data. Once we saw items that could become major issues for us, we were able to remediate potential problems right away."
>
> *- Steve Scott*
> *Information Security Manager*
> *SCHS*

Enabling Care Providers While Confidently Protecting Patient Data

ST. CHARLES HEALTH SYSTEM (SCHS)

St. Charles Health System (SCHS) is a healthcare delivery system comprised of three hospitals and some twenty clinics located in Central Oregon. With nearly 3,000 caregivers, SCHS provides a full range of medical specialties and services.

STARTING WITH A RISK ASSESSMENT

SCHS's CIO and IT department undertook a Baseline Security Risk Assessment since the organization had not conducted an independent, third party evaluation of their security posture in the past. Based upon a recommendation, they engaged CynergisTek, an authority in healthcare information security management consulting services and solutions. As part of their engagement, CynergisTek organized a two week Data Loss Risk Assessment, using the Digital Guardian for Compliance appliance.

The assessment consisted of installing the Digital Guardian appliance in a passive mode to monitor network transmissions for sensitive data. "Within literally minutes of the appliance being plugged in, we started collecting data. Once we saw items that could become major issues for us, we were able to remediate potential problems right away," said Steve Scott, Information Security Manager. "Because of the DG tool, we were able to identify issues and correct them before stringent breach notification laws were put into effect," said Scott.

After reviewing the results, SCHS's IT team became aware that there were two major communication channels that required immediate attention:

1. One of SCHS's hospital information system vendors had set up a secure point-to-point FTP channel over which the two companies would communicate. However, the vendor misconfigured the system. As a result, data was actually being sent out via the Internet instead of over the secure channel.
2. Various business associates (e.g. coders, insurers) were processing sensitive data and emailing it back to SCHS using unencrypted clear text messages.

When CynergisTek and Digital Guardian presented the findings, SCHS immediately addressed the areas of concern.

IMPLEMENTING THE COMPLETE DATA LOSS PREVENTION SOLUTION

Based on the successful Data Loss Risk Assessment, SCHS decided to implement the complete Digital Guardian compliance solution for on-going monitoring, blocking and discovery. They purchase and deploy two Digital Guardian Content Inspection appliances to provide DLP protection for all of their facilities.

DIGITAL GUARDIAN®

> Since implementing this data loss prevention solution, we find people are much more careful with the organization's sensitive data. We can give functionality back to our users knowing that our data is being properly handled and protected.

St. Charles HEALTH SYSTEM

- Steve Scott
Information Security Manager
SCHS

The appliances arrived preloaded with a wide range of HIPAA code set and healthcare EDI protocol identifiers, and preconfigured policies, including: ICD-9, LOINC®, NDC, SNOMED CT®, HCPCS, HL7 and X12. St. Charles Health System simply needed to register their sensitive data/documents and then activate one or more of the preloaded policy and reporting templates to begin detecting sensitive healthcare data leaks over the network.

"The appliances were easy to set-up and configure," said Steve Scott. "They worked just as advertised. We were up and running in an hour with the basic information in place to begin monitoring our systems."

RESULTS

Although SCHS already had policies in place regarding the handling of sensitive data, it wasn't until after implementing the Digital Guardian solution that they had the ability to effectively enforce these regulations.

"Our strategy is about educating employee and business associates' behavior through the policies we've set-up. We use Digital Guardian to supervise and reinforce the behavior," said Scott. "Since implementing this data loss prevention solution, we find people are much more careful with the organization's sensitive data. Having this tool enables us to not be the IT Police. We can give functionality back to our users knowing that our data is being properly handled and protected."

Minimal IT time is needed to maintain the system. According to Scott, responding to alerts and refining policies, as management identifies new data to be registered, is all that's required from him and his team. He finds himself spending less then 30 minutes a day with the system. The discovery component of the Digital Guardian has allowed SCHS to find and identify sensitive data stored on shared drives and desktops.

"We have found that people have legitimate sensitive information in areas they don't even know about," said Scott. "Once we discover this data we immediately move it into an encrypted area and then work with the owner to see if it's something to be stored or removed."

SOLUTION "WORKS JUST AS ADVERTISED"

Scott said that he was incredibly pleased with the overall solution as it works "just as advertised." He added that the support that he receives from both Digital Guardian and CynergisTek is "stellar."

St. Charles Health System is extremely committed to protecting the sensitive information of its patients, physicians, and employees. The organization continues to assess and refine their security infrastructure to ensure that this PHI is protected from accidental or malicious activity.

DIGITALGUARDIAN®

www.digitalguardian.com