DataMotion /SuccessStory

Stillwater Medical Center

Automatic Email Encryption for PHI boosts HIPAA / HITECH Compliance

For more information / 1.800.672.7233
info@datamotion.com

DataMotion /SuccessStory

Stillwater Medical Center

CHALLENGES:

- Protect healthcare communications
- Minimize false positives from content filtering
- Compliance with HIPAA/HITECH for Protected Health Information (PHI)

SOLUTION:

DataMotion SecureMail Gateway

"We are much more confident that sensitive employee emails are encrypted and in compliance with HIPAA/ HITECH regulations"

- Cliff Hanks, MCSE, GSEC, Senior Network Engineer, Stillwater Medical

Background

The Stillwater Medical Center is a non-profit accute care general hospital in north central Oklahoma and has been selected 3 years in a row as one of *Modern Healthcare's Top 100 Best Places to Work in Healthcare*. The 119 bed hospital is a regional health center for the area, providing a full range of services for its patients.

Located in Stillwater, Oklahoma, the Medical Center's systems and information technology staff report to the Chief Information Officer and include 12 systems analysts and 8 technical support analysts. Stillwater uses a Microsoft Exchange on-premise email server managed by their in-house IT group.

Requirements

Stillwater Medical needed a solution that would:

- Ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act
- Automatically monitor all employees' email communications for PHI (Protected Health Information) and encrypt as needed
- Reduce the risk of false positives (unnecessary encryption)
- Eliminate the need to exchange certificates
- Be simple to implement and administer with no need for recipient software
- Be intuitive to use for recipients and users
- Protect the organization's reputation and brand

Challenges

Stillwater Medical had been a longtime customer of the DataMotion SecureMail desktop solution. Prior to switching to SecureMail Desktop, users and recipients often had to exchange certificates making email encryption difficult and cumbersome or IT staff would create password protected, self-decrypting executable files for users to send as email attachments. SecureMail Desktop gave selected employees the ability to choose to encrypt certain email messages containing PHI on an as-needed basis and was very easy to use and IT staff no longer needed to create executable files to enable the secure transmission of PHI.

However, with HITECH giving HIPAA regulations more 'teeth' (including OCR audits) the hospital wanted to expand their usage to automatically monitor all of their outbound email for PHI. A risk analysis showed that installing a DLP (Data Loss Prevention) system would be a cost effective solution.

"The ability to customize email filtering has virtually eliminated false positives, and it's easy to update and change the filtering rules." – Cliff Hanks, MCSE, GSEC, Senior Network Engineer, Stillwater

DataMotion /SuccessStory

Solutions

Stillwater Medical decided to layer automated filtering encryption on top of the manual encryption provided by SecureMail Desktop and expanded its use of DataMotion technology across the entire organization by adding the DataMotion SecureMail Gateway as a DLP (data loss prevention) email filter. The Gateway automatically identifies emails that contain PHI (catching those messages employees forgot to excrypt) and automatically sends them on, encrypted. Now email content and attachments from the hospital's employees are automatically scanned for PHI, and automatically encrypted when needed. The system also automatically provides feedback, notifying users when something should have been encrypted, increasing email security awareness. "DLP is the name of the game for protecting healthcare information. For a hospital our size, to be able to do this so easily, the payback's enormous," said Cliff Hanks senior network engineer for Stillwater Medical. "We are getting the benefits of a larger hospital's technology, with a smaller amount of resources. It's great for security and compliance."

The SecureMail Gateway offers powerful, customizable, rule sets, which allowed the hospital IT staff to configure rules based on their own internal policies and needs. For example, custom pass rules have been used to alleviated false positives, which occurr when business partner account numbers also matched patient id numbers.

Stillwater Medical also implemented the SecureContact.me feature of SecureMail, enabling individuals outside the hospital's email sytem to easily send employees senstive information and files, without the need for additional software or services. "Implementation was simple and took very little time and effort to set up," said the senior network engineer.

Results

- Greatly reduced PHI exposure from email communications
- Increased compliance with HIPAA/HITECH regulations
- Reduced false positives, increasing user confidence and satisfaction
- Security enforcement is now measurable. Significantly reduced IT resources needed for outbound email security administration

"Our risk exposure has been significantly reduced by automating and extending DataMotion SecureMail technology to all of our employees. We can now filter all of their messages and files to identify and encrypt sensitive financial, clinical, and other private information," said Hanks. "The use of the DataMotion industry standard lexicons and custom email filters has virtually eliminated false positives and the need for IT intervention. We've significantly reduced the amount of time it takes to manage our outbound email and are much more confident that our sensitive employee emails are encrypted when needed and in compliance with HIPAA and HITECH regulations."

FOR MORE INFORMATION CONTACT US

200 Park Avenue Florham Park New Jersey 07960 Tel: 800.672.7233 Email: info@datamotion.com www.datamotion.com