

Easy-to-Use Encrypted Email for a Dispersed Staff & Client Base

SPHERIS

For Shayne Langford, Director of IT operations at clinical documentation provider Spheris, the security of the protected health information (PHI) transcribed by the company's 5,500 medical language specialists is a central responsibility. Spheris' commitment to security can be seen in its Web-based technology platform, which features integrated voice and data capabilities protected by enterprise-grade encryption. The question, however, was how to keep PHI secure should it ever need to be transmitted via email, outside of the Spheris technology platform. Spheris required a workable solution that not only provided for increased protection of PHI, but was also easy enough for the company's large workforce (not to mention the company's more than 500 clients across the United States) to implement immediately without significant training delays.

"When we started our email encryption evaluation process, we established four objectives," said Langford. "First, we must be able to guarantee to our clients that we are implementing the best possible systems to help ensure that any email with PHI is secure. Second it must provide a workable solution taking into consideration our commitment to comply with the HIPAA regulations. Third it must be an enterprise-class solution able to encrypt email within Spheris and scalable to our clients and their clients. And finally, it must not change the established email experience for the end users. In other words, we didn't want a solution that would entail the time-intensive and training-intensive process of rolling out client-side software to our client base."



ABOUT SPHERIS

Based in Franklin, Tenn., Spheris is a leading global outsourcing provider of medical transcription technology and services to more than 500 health systems, hospitals and group practices throughout the U.S. More than 5,500 professional Spheris medical language specialists support the company's clients through secure networks, using a Web-based system with integrated voice, text and data.

THE CHALLENGE

- ▶ Promote and support compliance with HIPAA regulations regarding protected health information using an enterprise-class encryption solution.
- ▶ Implement a secure messaging system within Spheris that would also be extensible to its entire client base.
- ▶ Find an easy-to-use encryption system that did not require the end user to go through time-intensive training on how to utilize the system.

THE SOLUTION

- ▶ Voltage SecureMail with Zero Download Messenger supports Spheris' commitment to adhere to HIPAA-protected health information requirements.
- ▶ Email containing sensitive information is automatically identified by Spheris' CipherTrust IronMail appliance and encrypted by Voltage, preventing disclosure of private health information.
- ▶ Voltage's automated key-management and easy-to-use interface allows Spheris employees to use their same familiar email interface and workflow tools, and precludes the need for extensive user training.

Supporting Better Healthcare

A leading global provider of medical transcription technology and services, Spheris supports more than 500 health systems, hospitals and group practices across North America. The company delivers a range of solutions to help facilities manage transcription and clinical documentation with an emphasis on verifiable quality, fast turnaround times and pricing. Spheris solutions enable doctors and other clinicians to input dictation using a telephone, PDA or PC. An onsite server collects all dictation files, which are then securely distributed to Spheris' network of more than 5,500 professional transcriptionists and editors, most of whom work from home. Spheris transmits sensitive sound- and text-based transcription files using technology that is safeguarded with private frame relay connections and secure VPN access with 168-bit encryption. As such, email doesn't usually enter the picture. However, when transcriptionists have questions about their work, they elevate the issue to a manager, who then interfaces with the client—often using email.

“To support our HIPAA compliance commitment, we evaluated and selected Voltage Security to guarantee our clients that we are implementing the best possible systems to help ensure that PHI is being protected during email transmissions.”

“It is not our normal business practice to send transcribed medical documents via email, but we realized that through the course of everyday business there was the possibility that PHI may be transmitted in an email,” explained Langford. “To support our HIPAA compliance commitment, we evaluated and selected Voltage Security to guarantee our clients that we are implementing the best possible systems to help ensure that PHI is being protected during email transmissions.”

Using the four objectives outlined above as its main criteria, Spheris evaluated several email and data encryption products. Langford and his team quickly found that while some of these products could meet one or two of their objectives, only Voltage met all four. According to Langford, there was also one final criterion that “led to our selection of Voltage” as the platform used to protect emails sent between Spheris personnel and physicians and administrators throughout the company's client base. “With Voltage, we didn't have to go touch every client,” said Langford. “In other words, we didn't have to download, install and manage client software for all our users. That was a decisive issue.”

Automatic Encryption Based on Key Words

The Spheris deployment features Voltage SecureMail with the Zero Download Messenger coupled with a CipherTrust IronMail appliance, which is customized for scanning for PHI information based on specific HIPAA regulations. If an email comes through that contains a social security number or other types of sensitive information, it is automatically sent from the CipherTrust box to the Voltage solution for encryption. This takes the decision-making out of the hands of any one individual user and significantly improves the maintenance of data privacy. In addition, Voltage's IBE technology offers superior key and policy management capabilities in comparison with conventional PKI-based encryption offerings. In fact, Voltage makes individual certificates superfluous and ties security policy directly to the encryption or authentication method. This eliminates the complexity of certificates, while still ensuring authorized key issuance and data integrity, and a level of security comparable to traditional encryption solutions.

A browser-based interface for two-way secure communication, Zero Download Messenger enables organizations to securely trade email and file attachments with customers and partners without them having to download or manage software on their desktops. Browser-based functionality also means that users can send secure messages and attached files to other individuals regardless of the email platform on the receiving end. Additionally, while many browser-based solutions require users to view their secure messages in a separate webmail system, Zero Download Messenger keeps messages where users expect them—in their inbox. The result is that end users can continue to use their same familiar email interface and workflow tools, and network administrators do not have to manage a separate, heavyweight mail infrastructure.

Spheris made it known that not forcing people to change the way they work and minimizing the need for encryption training were both very important goals. So Langford and his team created a simple set of step-by-step user instructions that they attach to the bottom of an encrypted email and send out to new users.

“Our administrators and health information managers are the primary users of secure email. Voltage Zero Download Messenger is very efficient and easy for them to use. As a result, it basically eliminated the need to train our administrators and health information managers on how to use email encryption,” said Langford. “And, we don't need to slow down our editors and operation supervisors; they just keep working and encryption happens automatically in the background. Voltage also allowed us to customize the look and feel to the Spheris brand. All together, these capabilities are invaluable in helping new users get up and running quickly.”