Secure Messaging in Healthcare: Tech Solutions for HIPAA-compliant Messaging

Save to myBoK

by Bob Janacek

Picture this scenario: a therapist receives an e-mail from a patient describing a set of symptoms and asking for advice. In another profession, the therapist could just whip off a reply. However in this profession, a well-meaning therapist who uses e-mail to dispense clinical advice just might be violating the law. Such is the nature of life in the healthcare business in the first age of technology.

These complexities have caused some healthcare providers to forbid employees to use e-mail to communicate with patients. Patients, however, have different expectations.

Patients want to communicate with their doctors through e-mail. They can organize the questions they want to ask, they can look up the names of their medicine, they can capture the answers the doctor provides—in general, it can be more convenient than a phone call or an office visit.

And patients don't understand why they shouldn't be able to e-mail—it's their own personal health information, and it seems as if they should be able to disclose or withhold it as they please. However, the situation is not nearly that simple, and healthcare providers do not have that freedom.

Fortunately there are effective methods to provide e-mail security for healthcare users. In order to use them, it is first necessary to understand how HIPAA regulates messaging.

HIPAA and ePHI

HIPAA's privacy and security rules cover a significant amount of information processed by healthcare organizations. It defines ePHI as any digitally transmitted information that identifies a person and includes information such as the person's physical or mental health, healthcare-provided demographic information, and payments related to healthcare.

HIPAA deems information identifiable if it includes information such as the patient or health plan member's name, address, significant dates, phone or fax numbers, e-mail address, identifying numbers, biometric data, or other unique physical characteristics. (Visit www.hhs.gov/ocr/hipaa/finalmaster.html for more information about identifiable information in the privacy rule.)

HIPAA requires the implementation of security mechanisms to protect ePHI from unauthorized disclosure. Encryption is not optional. The rule specifies it as a topic that must be addressed. Organizations covered by HIPAA are required to either implement encryption as stated in the rule, implement an alternative solution that provides equal protection, or sufficiently document why encryption will not be adopted. Cost cannot be the sole reason for not adopting an addressable implementation specification.

Much has changed since the HIPAA security rule took effect in April 2005. At that time encryption applications, such as those for e-mail, were expensive and not considered mature. That is no longer true. Now any organization covered under HIPAA must adopt the encryption implementation specifications included in the HIPAA security rule.

ePHI and Messaging

Systems such as e-mail and instant messaging are as pervasive in healthcare organizations today as they are in any other business. Healthcare employees use them in their daily routines, often working with messages containing ePHI.

Applications such as accounting systems are integrated into the organizational e-mail stream and require a patient's personal information in their use. New medical diagnostic systems generate huge electronic files containing vast amounts of ePHI. External consumers and vendors often need to initiate a secure message with the organization. To remain competitive on cost and service, organizations require the advantages of secure messaging between their employees, partners, and customers.

For that reason, organizations face a challenge in protecting ePHI without limiting their operational capabilities. An antiquated solution would be to block all messages containing ePHI; the unfortunate consequence would be that the work of busy and well-intentioned employees slows down. Successful organizations have implemented technology that protects their patients' privacy and supports transparent, secure data exchange.

The messaging industry has developed a set of streamlined, fully mature solutions that support the secure exchange of ePHI. The most interesting ones use multitenant software-as-a-service (SaaS) architectures that enable organizations, large and small, to transmit intranet and Internet messages that are HIPAA-compliant. These systems place a button in the e-mail client that gives the user the option of sending a secure message with no additional effort over sending an ordinary one.

SaaS systems (both hosted and in-house) enable even large organizations to rapidly deploy this functionality. This has eliminated any reason for an organization to worry about security when sending an e-mail to patients, exchanging medical information in-house, or sharing information with medical business partners such as insurance companies.

Message Encryption

Beyond the basic facts of messaging itself, secure messaging requires a deeper look into each individual message. The core issue of e-mail and ePHI revolves around how the message is delivered over the Internet. In order to comply with privacy laws, an organization cannot send sensitive messages in plain text. Encryption, however, has never gained widespread adoption. In the past, part of the barrier to its widespread adoption has been the technical nature of its user interface. Fortunately, this is no longer the case.

As the Internet has matured, many standards have been developed that can protect messages and large files containing ePHI. The end result is message privacy delivered to end users in as transparent a manner as possible. These standards include infrastructure technologies at the network level, integration technologies at the application server level, and encryption and document rendering technology already integrated at the client and handheld level.

One such standard, known as transport layer security (TLS), enables secure communication between e-mail servers and gateways. TLS is an ideal technology to leverage when business partner organizations need to send e-mail containing ePHI to each other across the public Internet.

In a similar manner, secure socket layer (SSL) allows Web servers to establish a secure connection with Web browsers, extending an organization's site to vendors and customers for the secure exchange of sensitive information. This allows Web site visitors to retrieve and reply to secure messages without special software other than an e-mail client and a browser. Online banking, stock trading, and Internet purchases use SSL.

Leveraging the encryption capabilities of SSL, Web services allow secure portals to integrate with back-end secure message data, allowing them to display a secure message center, for example, to the visitor who logs into their portal account. No additional credentials are required to view the secure e-mail, and the experience is completely contained in the existing portal.

It then makes sense to consider document formats that integrate security as part of their design. One of those formats is PDF. Adobe's Acrobat reader program, ubiquitous on client computers, serves as an excellent vehicle for displaying password-protected, encrypted documents representing sensitive e-mail content.

As an added bonus, PDF files are automatically compressed, decreasing the bandwidth requirements to access any embedded attachments such as Word documents or Excel spreadsheets. Encrypted PDF reading is already available for Blackberry and many other PDA users, allowing messages to be viewed securely when recipients are on the road.

Large files generated by medical imaging systems (often hundreds of megabytes in size) can be securely passed through e-mail systems by embedding a secure Web link. This allows recipients to download the files through their browser without proprietary secure FTP software. Automated batch jobs, such as invoicing, can be done by secure e-mail instead of postal mail. Messages containing ePHI can be tagged, for example, by adding “Secure:” to the message subject line. A content filter using predefined rules then securely routes these messages to the recipient.

There are additional benefits in integrating modern encrypted messaging systems with an organization’s various e-mail, imaging, automation, and portal systems. The result is greater ease of use for end users, as well as the opportunity for administrators to integrate many internal systems into a common secure delivery platform.

The good news is that by using encrypted messaging, organizations can meet the goals of regulation and provide appropriate privacy and security for patients, staff, vendors, and automated processes. These technologies are available today, packaged as in-house software or appliances, outsourced managed services, or a hybrid combination of the two. Compliance-based messaging offers organizations easy-to-deploy, mature services and software that enable the delivery of secure messages and require no user training.

Bob Janacek (bobj@certifiedmail.com) is CTO of CertifiedMail.com in Morristown, NJ.

Article citation:
Janacek, Bob. "Secure Messaging in Healthcare: Tech Solutions for HIPAA-compliant Messaging" *Journal of AHIMA* 79, no.6 (June 2008): 50-51.