

October 2002 - *Healthcare Informatics*

SECURE MESSAGING

Physician-patient email gathers steam

Like many of their colleagues across the United States, physicians at Lancaster General Hospital, Lancaster, Pa., are eager to exchange emails with their patients, hoping to use the Internet to facilitate communication and make face-to-face office visits more efficient.

But also like others in healthcare, the physicians are concerned about the security and privacy of their patient communications and about the potentially harsh penalties for failure under the Health Insurance Portability and Accountability Act (HIPAA).

For Terry Grogan, manager of information systems security at 550-bed Lancaster General, the goal has been clear--to find an IT solution that would securely enable physicians to communicate via email with patients, other physicians and hospitals. One challenge is that most vendor programs developed so far involve complicated public/private key management and other hassles. Fortunately, Grogan says, she and her colleagues located and have begun implementing a messaging solution, from San Mateo, Calif.-based Sigaba Corp., that provides for a secure "courier" system, which allows anyone in the system to initiate a secure email.

"If I have a radiologist who needs to get a radiology report to someone in the system, the traditional way to do that is by fax. But a lot of offices now are hooked up to the Internet and don't have faxes anymore," Grogan notes.

Now, once physicians are registered into the system, they can send or receive a radiology report as an email attachment. The Sigaba software automatically encrypts it, attaches a note assuring the recipient of its security, and asks the recipient for a Sigaba user name and password. Similarly, once patients have completed a one-time sign-up on the hospital's Web site, their replies to emails from Lancaster General are automatically encrypted, without the need for any special installations on their computer.

At the 138-bed Mission Hospital in the Mexican border region town of Mission, Texas, John Willars, director of information systems, had the same system installed. Initially, it was intended to help patient representatives respond more quickly to service complaints for patients still in the hospital. Mission's IT people had been "practicing sending emails from our physician representative to administration or other managers regarding patient complaints," Willars reports, "and they were using the patients' names and identification numbers." Now, with a secure email option, everyone's needs can be satisfied quickly, efficiently and securely--all at once.

Approaches to security

Though no one knows exactly how many patient care organizations are actively implementing secure email and messaging systems, there's no question that things are picking up steam, says Jeff White, a senior manager in technology services at Long Beach, Calif.-based First Consulting Group. It's apparent that hospitals, physician groups, integrated systems and health plans all want secure messaging--to satisfy consumer demands and physician, hospital and insurer needs. But challenges face the healthcare industry in this area.

"There are really two different markets" for secure email communications, White says. Hospitals need some kind of messaging/information flow with physicians and patients, and it needs to be encrypted. "It could be that encrypted email could be done through standard certificate solutions and programs," he notes. "But when it comes to patients, it becomes cumbersome and costly."

He sees two solutions: Rely on an email "push" system like Sigaba's, where no encryption certificates are necessary (and, to date, Sigaba appears to be the only vendor to have honed that approach). Or send unencrypted emails to patients and others outside the organization asking them to retrieve their new messages at the organization's portal--via secure communication on a Web browser with secure sockets layer. Organizations are trying out both solutions. White says he sees hospitals funding most secure messaging programs for physicians because of the investment involved.

Some vendors' strategies are based on that assumption. At Atlanta-based McKesson Corp., physician-patient messaging capabilities are part of a much broader approach. A "customer-service infrastructure" is being developed based on the concept of customer-service portals for patient communications and transactions of all types, says Connie Thompson, director of product management for McKesson Information Solutions. The company launched its Horizon WP Suite in late August.

Other vendors are going after the niche. For example, Emeryville, Calif.-based RelayHealth Corp. (formerly Healinx) continues to focus entirely on physician-patient messaging, says Eric Zimmerman, vice-president of product marketing. He's proud of the company's software, he says, which guides patients through a "virtual office visit." A series of questions for 36 common, nonurgent disorders help patients communicate quickly and efficiently with their physicians about current symptoms or follow up on an office visit (including prescription refills).

More than 3,500 patients and 300 physicians are using the application service provider-based solution. Zimmerman says that acceptance of such communications by health plans will help turn the tide toward broader adoption in the next few years. (Several major health plans already reimburse email messaging-facilitated virtual visits).

Some physicians are so certain of the advantages of secure messaging that they're developing their own software. Satish Kapoor, M.D., an internist and pulmonologist with the Heritage Medical Group in the New York City suburb of Sleepy Hollow, and his colleagues are working on a proprietary program under the company name xpressMDTechnologies. It's being beta tested and is set to launch commercially later this fall.

Hospital-based organizations are moving forward on multiple fronts. At Loma Linda University Medical Center, Loma Linda, Calif., for example, administrative director for the information security and HIPAA offices Alvin Siagian reports, "We have two-way pagers with email technology." Using technology from Alexandria, Va.-based Metrocall Inc., Siagian and his colleagues have expedited the process of paging physicians and nurses while also rendering such messages more secure through encryption.

Ease and convenience

Two technological keys to success in going forward with secure email will be "ease of adoption through leveraging of existing technologies that both parties have, and the delivery of meaningful data in a convenient way," says Jon Zimmerman, vice president of e-health for Malvern, Pa.-based Siemens Health Services. Siemens has partnered with Sigaba to provide messaging services to its clients. The logic of secure email is unstoppable, he says. After all, email is "the number one killer app in the online world," and over time, more vendors will figure out a variety of clever solutions to the technical and procedural challenges involved.

Zimmerman sees a point coming in the next couple of years when numerous patient care organizations will move to secure email. "If Boeing is sending CAD-CAM drawings of their next-generation airplanes securely through the Internet," he asks, "why can't healthcare do the same kind of thing?"

Mark Hagland is a contributing writer based in Chicago.
