Lowering Costs, Protecting Data through Content-based E-mail Encryption

Save to myBoK

by John Dasher

DeKalb Medical Center, a not-for-profit hospital system in Decatur, GA, that serves approximately 500,000 patients annually, was looking for a way to secure HIPAA-covered personal health records. “We wanted to eliminate any potential risk of confidential information leaving the facility electronically,” says Sharon Finney, information security administrator at DeKalb. “We were looking for a solution that allowed us to monitor and secure outbound e-mail traffic, but many solutions used proprietary mechanisms or didn’t offer encryption at all.”

In a related project, DeKalb also needed to transfer confidential financial, patient, and billing information securely to accounting and market research companies as well as third-party billing and collection companies. According to Finney, who is responsible for all business and clinical information on all systems and networks, some of the files were very large and contained confidential information, such as service and procedure codes, Social Security numbers, billing information, account numbers, medical record numbers, and demographic information.

“Our partners were only allowed to transfer data through a virtual private network [VPN] connection,” Finney explains. “It was difficult to manage and left information unprotected while stored on our file transfer protocol [FTP] servers. There was also a chance that someone could gain access to another person’s account or that we might put a file into the wrong folder by mistake.”

The Solution

DeKalb decided that it didn’t want to use a proprietary e-mail encryption solution such as those offered by many content-filtering vendors. “Instead, we wanted to use an industry-standard solution a lot of our partners already used-a solution that would also be accepted outside of the healthcare industry,” says Finney. DeKalb decided on implementing a content-based encryption system.

Compliance and Privacy as Drivers

HIPAA compliance and information privacy concerns were the main drivers for the two projects, which were sponsored by the compliance and information technology departments. “In the past two years, the Joint Commission has increasingly asked how we’re protecting patient information at rest and in transit, which we also need to detail in our annual audits,” Finney explains. “The Joint Commission has reported breaches in nine hospitals. The courts decide whether a breach occurred due to human error or to negligent security policy. If they determine negligence is the reason for a breach, the fines can be huge. Basically, we needed something that would stand up in court,” she notes.

The system provided a server-based architecture that centrally handles all key management, corporate encryption policy, and network infrastructure interaction for multiple applications. With the primary infrastructure in place, organizations can then integrate new encryption applications quickly and easily. This approach reduces the complexity of a security infrastructure, lowers maintenance costs, and results in good return on investment over time.

The Benefits of E-mail Encryption

DeKalb realized a number of benefits from implementing the system. As the IS administrator pointed out, “this system allowed us to deploy a solution that didn’t require anything to be installed on the recipient’s desktop. It gave us the flexibility to exchange data securely with recipients that used similar platforms as well as with those partners who didn’t have any encryption solution.” DeKalb’s content-filtering mail transfer agent (MTA) filters e-mails for spam, malicious content, and sensitive information. E-mails with sensitive information are routed to the universal server, which encrypts the contents and delivers them to external recipients. This setup eliminates the need for end users to classify information and ensures that all e-mails with sensitive content are always secured.

DeKalb also decided to phase out the VPN solution for its FTP servers and replace it with file encryption. “There was no question about whether we would use this technology to encrypt our files,” Finney says. “We use the program to encrypt files before they’re loaded onto the FTP server, which protects them both in storage and in transit so we no longer need additional transit protection such as a VPN. Equally important, this level of encryption is an industry standard and was very well accepted by our partners. They can opt either for an automated solution or choose an inexpensive, manual option if they only receive information sporadically.” Finney says another benefit is that if the FTP server is breached or a file accidentally ends up in the wrong folder, the files are still encrypted and the data are secure.

Finney says that before deployment, some departments were afraid encryption was going to complicate the communications process and handcuff them from a partner perspective. To address these concerns, the IS group put together a document for prospective partners that explained the hospital’s encryption standards for e-mail and FTP. “For e-mail, partners only need to install a client if they want to physically receive the file in their inbox,” she notes.

DeKalb will also move the FTP server out to a neutral zone between its private network and the outside public network to allow access without a VPN connection. “For FTP, partners are usually happy to purchase the program to secure the connection because they’re easier to use than a VPN, eliminate a step in the process, and provide a more stable connection,” she says.

Enhanced Customer Service

Another benefit of the system is enhanced customer service. “Before we introduced this system, our customer service department was not allowed to transmit patient information by e-mail even if the request from the patient came in by e-mail,” Finney says. “Instead, customer service had to pick up the phone and call them. Now, the combination of our content-filtering MTA and encryption software allows them to answer requests directly by e-mail. They can even have extended ‘conversations’ with patients and physicians via e-mail and include account numbers and codes without having to worry about whether it needs to be protected or whether it’s confidential.”

The IS administrator is now seeing an increase in e-mail traffic. “DeKalb Medical Center actively promotes the use of e-mail by patients to communicate with the medical center. This capability means more choice for our patients and lower costs for us, so it’s a great deal for both sides,” Finney points out. “Our user response has been very positive. Employees love the fact that they can e-mail without having to think about whether something needs to be secured.” Finney has also benefited. “Because users no longer have to ask what information is confidential, my call volume has decreased. We now have a tool that does this job, and it’s doing exactly what it’s supposed to do-very well.”

Finney is very satisfied with the outcome of the project: “If I were to do this project again, I wouldn’t do anything differently. It was probably one of the best and most seamless implementations we’ve done. The solution came in, and three days later we were encrypting e-mail. It was much easier than we’d anticipated.”

According to Finney, DeKalb Medical Center is looking at automating certain tasks in the future. “We’ve started to send out appointment information to patients via e-mail, and we can now include instructions such as whether they could eat before a certain medical procedure without worrying about keeping that information confidential. This capability will make the process more cost-effective and create a better information exchange with patients.”

John Dasher *(dash@pgp.com) is the director of product management for PGP Corporation in Palo Alto, CA.*

Article citation:
Dasher, John. "Lowering Costs, Protecting Data through Content-based E-mail Encryption" *Journal of AHIMA* 78, no.1 (January 2007): 58-59.

Driving the Power of Knowledge