

Major University Finds Voltage SecureMail Delivers Value Beyond Basic Regulatory Compliance

The HIPAA privacy regulations are a concern for hospitals and medical offices of all sizes. But for one large U.S. university that maintains a highly regarded medical school and two distinct teaching hospitals, the complexity and scope of its HIPAA challenge was very large indeed. To get out in front of this challenge, university officials began planning their compliance strategy more than a year before the HIPAA Security Rule came into effect in April of 2005. A central element of their plan was to establish a secure messaging capability.

“We provide email services for 25,000 to 30,000 faculty, staff and students,” explains a project manager from the university’s central IT organization. “Our top HIPAA concern, of course, was enabling medical school people to protect private health information. But since we manage the general email system for the entire university, it would have been difficult to isolate the hospital and just the email coming into and out of the medical department. Which is why we decided it would make more sense from both the compliance and administrative standpoints to roll out a secure messaging capability across the whole organization.”

“We tested three products that use encryption to protect emails and email attachments, and found that Voltage SecureMail combines the greatest ease of use with a very innovative key management approach.”

With such a large implementation, the primary criteria for the university’s secure email system were that it be simple to use and that it would work with any kind of email software, but not depend on or require a major investment in key management and disaster recovery infrastructure. “With so many users to support within the university, there really was no way for us to provide in-depth training, so the secure email system had to be extremely intuitive,” says the project manager. “We tested three products that use encryption to protect emails and email attachments, and

EXECUTIVE SUMMARY

When a large U.S. university began planning its HIPAA compliance strategy back in 2004, its IT staff determined that the most effective way to address the challenge was to implement a secure email system across the entire organization. The decision was initially prompted by technical considerations, but university officials hoped that the system-wide implementation would be embraced and add value beyond its medical and healthcare-related departments. In the years since the initial launch of the service, that’s exactly what is happening.

CHALLENGE SUMMARY

- ▶ Find an effective secure email solution to ensure compliance with HIPAA privacy regulations.
- ▶ Implement secure messaging that would allow faculty, clinicians and students to use encryption without changing the way they were using email already, or require extensive user training.
- ▶ Ensure low total cost of ownership and minimal administrative load through an advanced approach to encryption key management.

BENEFIT SUMMARY

- ▶ The Voltage SecureMail solution helped the university meet all HIPAA compliance requirements, including access and audit controls, and benchmarks addressing integrity verification, entity authentication and transmission security.
- ▶ Voltage SecureMail provides automated email encryption for all university staff, regardless of the software or operating system they use.
- ▶ Voltage-powered secure messaging also enables the university’s development department staff to safeguard the private financial information of alumni and benefactors donating money to the university.

found that Voltage SecureMail combines the greatest ease of use with a very innovative key management approach.”

Easy Enough For Everyone To Use

Voltage SecureMail was a perfect fit for the university on several levels. The university embraces a decentralized business model, which allows for distinct entities within the organization to maintain their own software, systems and processes. Hence, there is a great deal of diversity in the kinds of email software used. Voltage SecureMail excels in this type of situation because it is completely agnostic in terms of email client software and operating system. This meant that Linux-using grad students in the engineering department, Mac-using undergrads in the art department and Window-using doctors on the medical school faculty all could take advantage of Voltage SecureMail to send and receive encrypted email.

In fact, the university’s IT professionals worked closely with developers at Voltage to customize the solution for seamless functionality across all kinds of email programs. The result is that anyone within the university who wants to send an encrypted email—with or without attachments—simply has to include a key word in the title line of the email. When that message passes through the Voltage SecureMail Gateway in the university’s central IT office, it is automatically encrypted as it leaves the network edge.

“Other than knowing to type the key word in the subject line, there’s really no learning curve for our users,” states the university project manager. “We wanted to empower them to take the initiative to ensure HIPAA compliance on their own through their day-to-day work processes. Voltage SecureMail made that possible.”

“We wanted to empower them to take the initiative to ensure HIPAA compliance on their own through their day-to-day work processes. Voltage SecureMail made that possible.”

While some encryption products are targeted around narrow regulatory requirements, Voltage SecureMail enables organizations to address all the technical safeguards of a HIPAA-compliant secure messaging system. These include access controls to confirm that email senders and recipients are in fact who they claim to be, and audit controls to log all

user activity so that organizations can prove the message was sent securely, identify suspect data access activities, and respond to potential weaknesses. Voltage solutions also incorporate digital signatures to verify that messages reach their recipients unaltered and unchanged, and personal and entity authentication too. This innovative capability allows for encryption keys to be generated using simple identities such as an email address or network logins.

Furthermore, Voltage’s Identity-Based Encryption (IBE) enables data to be encrypted without the need for certificates. As such, Voltage solutions are far easier to manage than conventional encryption systems, which require extensive infrastructure and personnel to manage certificate revocation lists. “Competing encryption offerings we looked at would have required us to hire three or four dedicated administrators to keep everything running smoothly,” relates the project manager. “Voltage can be managed with our regular email administrative staff, saving us a lot of time and money.”

Not Just For Compliance

When university officials made the decision to provide encrypted email capability to everyone on campus rather than strictly among those directly impacted by HIPAA, the expectation was that other valuable uses would be found for secure messaging. Again, the thinking was that if the secure messaging capability were easy to use, people would be more likely to make it a part of their day-to-day routine. One area where the technology has been enthusiastically embraced is in the university’s development office.

The department responsible for raising funds to support campus initiatives, the development office often handles sensitive financial information provided by alumni and campus benefactors. “Development office staffers have told me that they often had to avoid email in the past because they didn’t want to expose donors to any kind of privacy breach,” explains the project manager. “With a secure email channel, our development professionals can start using email again with the confidence that they are protecting people who give to the university. Whenever they have to exchange private financial information among themselves or with outside institutions, they know that Voltage SecureMail ensures the privacy of all the stakeholders.”