



SENDMAIL.

Case Study: Healthcare Patient Confidentiality is Safe with Sendmail.

Industry	Healthcare
Company and Location	An Ivy League University Medical School affiliated with one of the largest Hospitals in New York, New York USA
Business Need	Email system that provides secure communications for transmitting confidential patient data (as mandated by HIPAA Act of 1996).
Solution	Sendmail Mailstream Manager <ul style="list-style-type: none"> - 1 Sendmail Multi Switch and 4 Managed Switches with Transport Layer Security (TLS) encryption - LDAP integration - MIME email attachment filter
Results	Sendmail created a flexible and secure Internet mail system that provides secure email communication between mail servers and in-boxes.

Overview

Since 1898, this University medical college and teaching hospital has been among the top-ranked clinical and medical research centers in the country. With its geographically broad healthcare system covering New York, New Jersey and Connecticut, dedicated staff, modern facilities, state-of-the-art technology, and commitment to quality care, it has become a model of innovation for medical institutions in the adoption of technology to advance patient care. With the recent ruling by the Department of Health and Human Service's Standards for Privacy of Individually Identifiable Health Information (45 CFR Parts 160 and 164), both the school and hospital were required to comply with the secure communications provisions of this ruling. The Office of Academic Computing (OAC) for both entities was put in charge of developing a strategy for securing email communication between its 10,000 users, patients, partners and the email servers.

About HIPPA Privacy Ruling 45 CFR Parts 160 and 164

This privacy rule is the second in a series of rules mandated by sections 261-264 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191. In general, the Privacy Rule 45 CFR Part 160 and 164 establish standards which entities covered by the statute—health plans, health care clearinghouses and certain healthcare providers—are required to comply with and protect the privacy of certain individually identifiable health information ("protected health information"). The standards establish requirements relating to the uses and disclosures of protected health information, the rights of individuals with respect to their protected health information, and the procedures for exercising those rights. Healthcare providers must comply with this ruling no later than April 14, 2003.

Challenge: Conforming with new regulations while maintaining performance

With the HHS ruling in effect, the OAC initiated an email project to comply with the Privacy Rule and support the increased importance and use of email by the medical college and hospital. In essence, the email system must secure email in data flow, patient confidentiality and handling of messages that flow in and out of the mail system. Privacy of Internet mail must also be secured between mail servers and in-boxes for recipients and senders.

With new security requirements and email traffic and volume increasing to more than 30,000 messages per day, the OAC faced performance and system management issues that could impact the service levels expected by its users. And finally, this solution must integrate with the existing mail servers and Eudora clients already in use.

Objective: A secure and high performance Internet mail infrastructure

According to the Associate Director of the OAC, the goals for its security compliance and performance requirements issues were clear:

- Secure email communication—establish stable and reliable communications that meet the HIPAA Privacy Rule requirements.
- Integrate with the existing environment—easily integrate with the existing email servers and Eudora mail clients that interface with the email system
- Lightweight Directory Application Protocol (LDAP) integration to improve management of email accounts.
- Anti-spam and abuse tools—to protect their email environment against spam and unwanted attachment types.
- List management support—easy to use management tools to help the OAC manage over 600 lists in use by the university and hospital.

Solution: A secure and easy to manage Internet mail system from Sendmail

To reach the OAC's objectives, Sendmail recommended deploying Sendmail's Mailstream Manager solution at the Internet firewall boundary. This solution includes Sendmail Switch deployed in front of the existing mail server, Transport Layer Security (TLS) encryption to secure email transmissions and MIME attachment filter to protect their system against spam and unwanted message attachments.

- Internet gateway protection—Sendmail Switch was implemented behind the firewall for secure administration and at the firewall boundary for incoming mail. This implementation phase included LDAP directory support, SMTP authentication and TLS encryption between mail servers.
- Mail hub and mail routing—Sendmail was deployed in front of the existing mail server to route outgoing mail and function as the mail hub. According to the Associate Director, "Sendmail is the best implementation for Internet mail. While it may be possible to extend our existing system to do more than just mailbox hosting, it is in not good as an SMTP server. It does not handle high volumes for mail routing, spam features are unsatisfactory, and it is not very configurable; however, it works very well with Sendmail Switch."
- Lightweight Directory Application Protocol (LDAP) integration—Consolidating their user information in one repository enabled OAC to reduce management and maintenance time.
- MIME attachment filter—to filter out suspect attachments based on filter type.
- Web-based administration—With Sendmail's easy to use interface, OAC's administrators are able to manage and control the mail system from any location.

Results: The model for secure and robust Internet mail communications

Sendmail's secure Internet mail solution complies with the Privacy Rule and provides enhanced protection against spam and unwanted attachment types. It transformed an inflexible system into a robust communication tool that has become a model for other healthcare organizations. Patient confidentiality and security is achieved while management has the tools necessary to maintain and manage system performance.

- Secure email communications— Eudora, the OAC's mail client, has recently released an edition that supports TLS. The OAC plans to use the TLS support in Sendmail Switch to support compliance with HIPAA regulations.
- Web-based Administration Tools—UNIX administrators are now able to access the administration console from anywhere and the web-based administration console helps them save valuable time and has been used as a training tool for junior administrators.
- Anti-Abuse Control—prior to Sendmail, said the Associate Director, " we were throttled with spam on a daily basis. With Sendmail, we've reduced spam significantly by using the subject line filter and anti-spam controls to filter out spam,".
- Virus protection—the Sendmail MIME Attachment Filter provides a frontline defense to supplement virus protection. "We have been hit several times by viruses from outside emailers on Exchange and Outlook clients. The Sendmail MIME Attachment Filter will quickly filter out suspect attachments based on MIME Attachment type. We also plan to use the size restriction features to restrict attachment size to less than 2MB."

This top-ranked clinical and medical research center has standardized on Sendmail as their Internet messaging platform. The Associate Director of the OAC concludes, "If we need anything specialized, Sendmail solutions have the flexibility to accommodate just about anything to meet our requirements. Sendmail is helping us to comply with HIPAA regulations for patient privacy. The standards-based open source foundation provides a robust, extensible platform for a solid Internet mail infrastructure to build on."



SENDMAIL.

Sendmail, Inc.
6425 Christie Ave, 4th Floor
Emeryville, CA 94608

V: 510 594 5400 F: 510 594 5411
www.sendmail.com

©2002 Sendmail, Inc. All rights reserved. Sendmail, Sendmail Pro, and the Sendmail logo are trademarks of Sendmail, Inc. Other trademarks, service marks, and trade names belong to their respective companies. Information and specifications may change without notice.