

Mirapoint Meets the Needs of Healthcare

Secure Messaging Simplified

“PROVIDERS AND OTHERS IN THE HEALTHCARE INDUSTRY CAN DERIVE TREMENDOUS VALUE FROM THE USE OF EMAIL, BOTH AS A MEANS OF GAINING A COMPETITIVE ADVANTAGE AND THROUGH REALIZING THE OPERATIONAL EFFICIENCIES THAT EMAIL OFFERS.” OSTERMAN RESEARCH

INDUSTRY BRIEF | HEALTHCARE

- Provide reliable, highly available messaging services that enforce the authentication and encryption controls required by HIPAA
- Fully integrated technology protects networks from viruses, spam and other unauthorized traffic
- Provide the policy-based controls for blocking, redirecting and archiving messages, based on regulatory requirements and internal guidelines
- Greatly simplify network administration and reduce TCO with a single web-based management console

HIPAA compliance is a must for healthcare messaging services

Hospitals and healthcare organizations face a new set of requirements to assure patient privacy. The 1996 Health Insurance Portability & Accountability Act (HIPAA) has had a wide ranging impact on the way hospitals handle information, particularly electronic medical records (EMR). These requirements, which must be met by 2006, affect how hospitals secure their network and all of the services offered on the network; in particular, communication using email must be secure. The liabilities and penalties for failing to meet HIPAA requirements are frightening, up to \$250,000 in fines and imprisonment of up to 10 years. Given this reality, hospitals need messaging solutions that assure patient privacy and thwart all virus and spam attacks as well.

Mirapoint's secure messaging infrastructure solutions can help

Mirapoint, the leading secure messaging provider, offers messaging solutions that enable healthcare organizations to deliver a secure, scalable messaging infrastructure that meets the challenges of regulatory compliance. With Mirapoint, healthcare organizations can deploy a messaging infrastructure that includes email filtering and scanning of messages to detect content requiring special treatment. Such content would include all patient health information (PHI), including electronic medical records (EMR) appointment information, prescriptions, invoices and bills, American Medical Association (AMA) treatment codes, and Centers for Medicare and Medicaid Services (CMS) disease codes.

Mirapoint Meets the Needs of Healthcare

Secure Messaging Simplified

Mirapoint messaging appliances are the building blocks of an “always-on” messaging infrastructure that addresses security throughout the fabric of the network, not just at the network edge. A Mirapoint appliance-based infrastructure can easily scale to meet the growing needs of even the largest healthcare organizations while maintaining the lowest TCO in the messaging industry and providing a platform for the provisioning of new services. Mirapoint solutions are designed to meet the demands of the healthcare industry by providing:

- Proven five-nines reliability (less than 6 minutes of downtime per year)
- SMTP-layer edge blocking reducing unwanted message traffic by 60-80%
- 98% spam catch-rates with virtually zero false positives
- Integrated zero hour virus scanning technology
- Outbound content filtering for global policy enforcement and regulatory compliance
- Encrypted transmission of messages from client to the mail server
- Secure, hardened, operating system with no known exploits for extra protection against hackers
- Sender authentication to assure messages from unauthorized sources never enter the network
- Standards-based architecture works with major email clients (Outlook, Eudora, Netscape, etc.), legacy email applications, directory servers and storage options
- Collaborative services including calendaring, group scheduling, address book and to-do-lists
- Microsoft Outlook synchronization for a seamless end-user transition

Integrated, Secure Messaging Appliances

Message Server. Mirapoint’s appliance-based Message Server provides 99.999% availability with exceptionally high performance. Users can access their email from any desktop via a secure, web-based interface, or via any standards-based email client including Outlook. In addition to its email functionality, the Message Server also provides easy-to-use collaboration tools, including group calendaring, scheduling and address book.

RazorGate. Mirapoint’s RazorGate appliance is an award-winning security appliance that incorporates everything you need to ensure the security of your message networks. It blocks spam, protects against viruses, and filters content for both inbound and outbound messages. RazorGate is also a powerful router that can be used as a front end to integrate heterogeneous email systems.

Directory Server. The Mirapoint Directory Server appliance is the industry’s first high-performance appliance providing unified user and system management. With proven scalability to millions of entries, the Mirapoint Directory Server simplifies the creation, use and integration of LDAP directories as a common information database for all messaging and related applications. Like the RazorGate and Message Server appliances, the Directory Server is also fully compatible with other directory products, including Active Directory.

HIPAA Requirements	Functionality Needed	Application Approach	Security Approach	MIRAPOINT
Access control (context-based, role-based, user-based, or some combination of these)	Per group/per user/per role controls; secure web mail access			X
Authorization control (role or user-based) that ensures that healthcare information is made available only to authorized users	Per group/per user/per role controls; policy-based global administration			X
Data authentication (ensuring data integrity)	SMTP authentication	X	X	X
User authentication (includes three elements—automatic logout, unique user IDs, and an authentication feature such as a password or PIN)	Password protected login; LDAP integration	X		X
Audit controls (record system activity for analysis)	Outbound filtering; wiretapping; audit and forensics tools		X	X
Encryption of data (protect data from unauthorized eavesdropping; optional)	Support Server to client encryption	X	X	X