

Messaging in the Healthcare Industry



an Osterman Research white paper
sponsored by Vircom, Inc.



Why You Should Read this White Paper

Email is the lifeblood of most organizations – it is the single most important communications medium used by the majority of employees in organizations of all sizes.

Healthcare organizations, in particular, can make good use of email for two reasons:

Many healthcare-related organizations are reluctant to use email because they fear that confidential or otherwise sensitive information could be subject to interception by unauthorized parties.

- Email can make data transfer more efficient, thereby speeding the delivery of healthcare services and making everyone in the healthcare industry – physicians, insurance providers and patients – more productive and better informed.
- Unlike most other industries, email is not used nearly as widely by healthcare providers as it could be due to concerns about the security of email, spam and other problems. Consequently, email can provide a competitive advantage to healthcare providers that use it effectively.

This document examines the role that email can play in making healthcare providers more efficient, as well as the key problems and regulations faced by healthcare providers as they consider using or expanding the use of email in their organizations.

The Role of Messaging in Healthcare

In many ways, the healthcare industry tends to be somewhat conservative regarding the use of messaging, often for good reason. Much of the healthcare-related information that would be sent through email is sensitive in nature: Social Security numbers, confidential health-related information and the like. As a result, many healthcare-related organizations are reluctant to use email because they fear that confidential or otherwise sensitive information could be subject to interception by unauthorized parties. For example, only 60% of medical personnel in healthcare organizations communicate with each other about patients using secure email, and only 28% communicate with each other about patients using non-secure email. This leaves the telephone as the primary method for medical personnel to exchange information about patients in real time.

However, healthcare-related organizations have a great deal to gain by using email and other types of electronic data transfer. For example, in a survey conducted by

Osterman Research in January 2005, it was discovered that nearly 60% of consumers consider the ability to communicate with a physician via email an important or extremely important factor in their choice of a physician, all other things being equal. Between healthcare providers, the ability to send information via email can dramatically speed the transfer of time-sensitive information, lower the cost of transferring this information, speed insurance claims processing and generally improve the level of healthcare service.

HIPAA is one of the most important concerns faced by healthcare-related organizations because of its far-reaching impacts on a wide variety of organizations.

Concerns About Email Use

In a survey conducted by Osterman Research in late 2004, it was discovered that healthcare-related organizations face a number of potential problems with regard to the use of email. For example, healthcare-related organizations had experienced the following problems during the six months prior to the survey:

- 91% had employees complain about spam.
- 71% had experienced the infiltration of a virus, worm or Trojan Horse.
- 21% experienced a denial-of-service attack.
- 14% had one or more email messages intercepted.
- 7% had one or more email servers hacked.

The Changing Regulatory Landscape

The healthcare industry has always faced significant regulations – many of which required records retention – but those regulations were generally not focused on electronic documents or messages. However, in 1996 the US Congress passed the Health Insurance Portability and Accountability Act (HIPAA), which includes new requirements regarding electronic records and communications. HIPAA is one of the most important concerns faced by healthcare-related organizations because of its far-reaching impacts on a wide variety of organizations.

What is HIPAA?

The Health Insurance Portability and Accountability Act addresses a number of different areas and one of its main purposes is to reduce administrative costs and burdens in

The real risk [with HIPAA] for most healthcare providers and related industries is that non-compliance can lead to loss of reputation, contracts or accreditation.

the healthcare industry, as well as the costs of government reimbursement programs, such as Medicare. Congress included provisions that specify the use of standard electronic formats for transmission, exchange and processing of administrative and financial data regarding healthcare transactions. HIPAA establishes standard electronic data interchange (EDI) formats for transactions and records such as benefit enrollment forms, medical claims and reimbursements, and health plan premium payments. It also establishes standard code sets (to replace proprietary and ambiguous codes) for medical diagnoses and procedures as they are coded for claims and billing.

Furthermore, HIPAA establishes standards for protection of patient privacy rights, including controls on access to and disclosure of personal data (protected health information, or PHI) inside or outside an organization.

Who Must Comply with HIPAA?

Firms that are subject to HIPAA regulations are called covered entities (CEs). These include:

- **Healthcare providers**
All hospitals, clinics and other firms that provide medical services.
- **Health insurance firms**
This includes providers of health plans.
- **Claims processing services**
Health care clearinghouses must comply.
- **Employers**
Large employers who self-insure or employers who provide health services may be subject to HIPAA regulations for those activities.

Penalties for non-compliance from Health and Human Services can include “civil monetary penalties” (fines) of \$100 for each violation, up to a maximum of \$25,000 for all violations of an identical requirement or prohibition during a calendar year. Furthermore, the US Department of Justice can prosecute for wrongful disclosures of protected health information (PHI). Penalties range up to 10 years in prison and a \$250,000 fine. The real risk for most healthcare providers and related industries is that non-compliance can lead to loss of reputation, contracts or accreditation.

What Does HIPAA Require for Messaging?

HIPAA does not focus on electronic messaging per se, but covers any type of record that contains PHI. PHI includes any details on an individual's physical or mental health, medical care, payment for care (e.g., insurance statements) or personal data (e.g., name and address) whether in paper or electronic form. Thus, any form of electronic messaging that contains PHI must conform to the HIPAA standards.

HIPAA does not focus on electronic messaging per se, but covers any type of record that contains protected health information (PHI).

HIPAA has two main components as it relates to these electronic documents: privacy and security.

- **HIPAA Privacy Rule**
This rule establishes standards for protection of patient privacy rights, including controls on access to and disclosure of personal data either inside or outside an organization. The privacy rule applies to paper records, as well as electronic records and messages and is designed to restrict access to individual health data, allowing the minimum necessary access.

- **HIPAA Security Rule**
This rule establishes standards and requirements to ensure confidentiality and integrity of PHI in electronic records during transmission and storage. The rule requires administrative, physical and technical safeguards:
 - **Administrative safeguards**
Requirements include establishment of a Data Backup Plan "to create and maintain retrievable exact copies of electronic PHI".
 - **Physical safeguards**
Requirements include device and media controls – policies and procedures that govern the receipt, movement and removal of hardware and electronic media that contain electronic PHI.
 - **Technical safeguards**
Requirements include access controls, such as unique user IDs and authentication, audit controls and encryption where appropriate (e.g., for transmission of PHI across the Internet). However, healthcare providers need to be careful about the encryption because there is a section that addresses the need to access critical information (i.e., decrypt) immediately in the event of medical necessity.

Healthcare providers, such as hospitals, must retain medical records under various laws and regulations – for five years, six years, the life of the patient, for two years after a patient’s death, etc. – and those records are subject to HIPAA privacy rules.

Clearly, the challenge for complying with HIPAA-related messages for most organizations is process, not quantity. For most organizations, typically, only a small fraction of email messages actually contain PHI. However, 100% of these messages must be managed per the regulations.

What Are the Deadlines for HIPAA Compliance?

The compliance deadline for the privacy rule was April 14, 2003. The compliance deadline for the security rule is April 21, 2005, and many large healthcare firms are currently conducting risk assessment, policy definition and architecture planning or deployment to ensure that they meet this deadline.

Other Healthcare-Related Requirements

The Medicare Conditions of Participation requires hospitals to retain medical records for five years. Medicare requires that medical records be retained for five years as they relate to radiological and nuclear medicine services and inpatient and outpatient services, among others. Psychiatric hospitals must also retain a variety of medical records for five years. Further, Medicare and Medicaid reimbursement to rural health clinics requires that these clinics maintain medical records for six years.

Issues with HIPAA

In a survey conducted by Osterman Research in late 2004, it was discovered that fewer than one-half of healthcare organizations are fully HIPAA-compliant, but that most of those that are not fully compliant are in the process of implementing security measures. However, despite the lack of full HIPAA compliance, the vast majority of organizations have ensured that policies exist to control access to, and release of, patient-identifiable health-related information.

Part of the reason for the lack of full HIPAA compliance lies in the fact that in many healthcare-related organizations there is insufficient knowledge about HIPAA requirements. For example, Osterman Research found that only 29% of healthcare organizations consider that they know all they need to know about HIPAA. However, three out of four

Fewer than one-half of healthcare organizations are fully HIPAA-compliant, but most of those that are not fully compliant are in the process of implementing security measures.

healthcare-related organizations employ an individual whose role and responsibilities are to implement and enforce HIPAA privacy policies and procedures.

HIPAA is Expensive

Becoming compliant with HIPAA does not represent a trivial expense: Osterman Research found that in healthcare organizations there is a median of two full-time equivalent staff members working on HIPAA-related tasks per 1,000 employees. If we assume that the fully burdened salary for each staff member is \$65,000 annually, then the cost of just labor alone for HIPAA-related compliance is \$130 per employee per year. Further, one in eight healthcare-related organizations has spent substantially more of their IT budget on HIPAA compliance, while another three in five has spent somewhat more because of HIPAA compliance. Only 26% of healthcare-related organizations have not spent more of their IT budget as a result of HIPAA.

There is a median of two full-time equivalent staff members working on HIPAA-related tasks per 1,000 employees.

What Healthcare Organizations Need

Healthcare-related organizations have a number of requirements when it comes to messaging:

- **A way to eliminate the vast majority of spam while generating very few false positives**
In the above-mentioned 2004 Osterman Research survey, 58% of healthcare organizations feel that spam is a serious or major problem – spam was identified as a more serious problem than even viruses and worms. Spam is a particularly serious problem in the healthcare industry because a number of terms that are commonly and legitimately used by healthcare providers – such as Viagra, Cialis and a variety of anatomical terms – are often used in spam messages, making false positives a serious problem for healthcare providers.
- **Protection from a variety of attacks**
Email, particularly when used to transmit sensitive information, must be protected against hacking, denial-of-service attacks and other attacks that could intercept confidential information. This is critical in order to comply with regulations like HIPAA, but also to make patients, physicians and others comfortable with and confident in their ability to communicate securely.

Spam is a particularly serious problem in the healthcare industry because a number of terms that are commonly and legitimately used by healthcare providers are often used in spam messages, making false positives a serious problem for healthcare providers.

An email system used by healthcare providers should provide a variety of deployment formats.

- **Ease of use**
Any email system in the healthcare industry must be very easy to use. Physicians and other healthcare providers simply do not have the time necessary to learn how to use new messaging systems, and patients simply will not use systems that have a high learning curve. Therefore, the ability to send information securely must be simple to learn and use.
- **Flexible deployment**
There are a wide range of organizations in the healthcare industry that need robust email capabilities, from large insurance companies with thousands of employees and a dedicated IT staff to small clinics with only a few employees. Therefore, an email system used by healthcare providers should provide a variety of deployment formats, including both software and appliance models for those that desire an on-premise solution, as well as hosted solutions for those providers that do not want to maintain their own email capability in-house.

Vircom Solutions for Healthcare Providers

Understanding that a substandard email infrastructure compromises patient privacy, introduces network vulnerabilities and hinders user adoption, Vircom develops secure email management solutions that safeguard the transmission and storage of electronic protected health information (EPHI) for covered entities in the healthcare industry.

A vital part of any risk assessment plan, Vircom's secure email management solutions offer customizable features and sophisticated filtering capabilities that coincide with the bilateral, secure data exchange channels created by Modus™. The combination of features and protected channels ensures uncompromised, flexible email environments for critical and day-to-day email communication.

Why Healthcare Organizations Use Modus

- Evolutionary email management and security features including encryption and archiving.
- Multi-level delegation features enable administrators to customize user settings according to access control policies.
- Airtight perimeter defense maximizes system performance by blocking obvious forms of spam that would otherwise require processing and burden the quarantine.
- Unparalleled false-positive protection ensures that legitimate emails and attachments containing health-related expressions are successfully delivered.
- Email auditing function lets administrators monitor compliance regarding the exchange and storage of protected health information.
- Customizable Sieve scripts allow administrators to influence engine behavior using specified filtering parameters that discern legitimate emails from spam.
- Three deployment possibilities (hardware appliance, software gateway, managed service) satisfy the needs of diversified organizational structures.
- Easy-to-install solutions reduce the learning curve to ensure fast user adoption and long-term satisfaction.
- Availability of clustered solutions support redundancy setups and ensure fault-tolerant email protection.
- Mature, award-winning technology backed by 10 years of industry expertise and professional services including 24/7 support.

About Vircom

Montreal-based Vircom is a leading developer of secure email management and authentication solutions for the demanding needs of Internet Service Providers, the real estate industry, corporations and healthcare. Vircom's mature Modus™ secure email management technology incorporates over 10 years of industry expertise, making it a powerful driving force in the defense against spam and email-borne fraud. Rated "Best Windows-based Anti-Spam Solution" by *Network Computing* and named a "2004 Recommended" product by *SC Magazine*, Modus has gained important industry recognition, including a record-breaking five-award distinction from *Windows IT Pro* magazine.

Vircom is also the developer of VOP Radius, a full-featured all-in-one RADIUS server that supports the latest RFCs, vendor specific attributes, NAS templates and has a multitude of preconfigured settings.

For more information visit www.vircom.com or call 1-888-4-VIRCOM.

© 2005 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed outside of Vircom, Inc., nor may it be resold by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

THIS DOCUMENT IS PROVIDED "AS IS". ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.