



Confidence in a connected world.

## **Managing Electronic Messaging and E-Discovery for Healthcare Providers**



# Managing Electronic Messaging and E-Discovery for Healthcare Providers

## Contents

<b>Executive summary</b> .....	4
<b>Introduction</b> .....	4
<b>Message management and e-discovery challenges</b> .....	6
<b>Identifying best practices</b> .....	8
<b>Developing and implementing a message management and e-discovery program</b> .....	9
Automatic, secure, and scalable message management .....	10
Efficient archiving .....	10
Improved content control .....	10
Elimination of personal storage and incorporation of legacy data .....	11
Message recovery in native formats .....	11
Open approach to e-discovery .....	12
Capability to enforce a litigation hold .....	12
<b>Message management and e-discovery program benefits</b> .....	12
<b>Symantec solution for message management and e-discovery</b> .....	14
<b>Conclusion</b> .....	14

## **Executive summary**

As corporate messaging systems grow, enterprises struggle with the complex task of not only finding sufficient storage space, but also ensuring that they can locate relevant messages from within that ever-growing mass. Healthcare providers face these same challenges and more, with their increasing reliance on email and other electronic communication, stringent legal discovery requirements, and patient confidentiality concerns.

Without effective message management, healthcare providers are vulnerable to financial and litigation risks as well as public relations damage. By establishing a comprehensive message management program, they can mitigate these risks as well as reduce storage and administrative costs; classify and tag messages to speed retrieval; and provide a quick, accurate, and less costly response to litigation discovery requests. An effective solution to meet message management, patient confidentiality, and discovery requirements couples a healthcare provider's business processes with high-technology solutions that can substantially reduce a provider's costs and risks.

Healthcare providers are also working to comply with regulatory requirements for document retention and maintenance, as well as new federal rules for fulfilling litigation discovery requests for electronically stored information, including email, instant messages (IM), and shared documents. Failure to comply with these new rules can impair a provider's ability to mount a strong defense in legal proceedings, jeopardize Joint Commission accreditation, damage public relations, reduce revenue, and risk failing to comply with an increasing number of state privacy standards.

One of a series that describes information technology best practices in the healthcare industry, this paper outlines best practices for coping with a healthcare provider's electronic message volume and for meeting litigation requirements under the new rules governing e-discovery.

## **Introduction**

In organizations of all kinds, email is becoming the primary means of business communication. Healthcare providers are not exempt—email is now commonly used to exchange confidential patient information between providers and patients, between providers and insurance companies, and along other pathways. Other communications programs, such as instant messaging, file-sharing applications, and enterprise resource planning (ERP) systems contribute to the rapid expansion of electronic communications.

## Managing Electronic Messaging and E-Discovery for Healthcare Providers

As these messaging systems grow, so do the requirements for storing and managing electronic messages, particularly email. Email servers have become critical to the mission of nearly all businesses, and the broad scope of email communication affects most aspects of business operations. Many organizations simply add more mail servers and use the servers as mass storage devices. According to a study<sup>1</sup> by Redgrave Daley Ragan & Wagner LLP, email volume will nearly double in the five years between 2006 and 2010, from 171 to 331 billion messages. And the messages themselves are larger: A typical corporate user creates 19.5 megabytes worth of email every day. Add instant messages and other electronic communications, and the volume grows even faster.

To cope with this growth, many organizations are adopting message management and archiving systems that index and retain a company's electronic communications. An essential component of comprehensive message management systems is a well-defined process for preserving and retrieving individual email messages. Yet according to a recent study, two-thirds of companies don't keep an accurate inventory of where their user data is stored.<sup>2</sup> And more than one-quarter of healthcare providers know that their organization needs to comply with requirements of the Health Information Portability and Accountability Act (HIPAA), but they are not fully compliant.<sup>3</sup>

Due to the nature of their services, healthcare providers are more likely than other types of organizations to receive requests for electronic communications—from patients and news media or as the result of litigation. To respond quickly and accurately to a request for electronic communications, healthcare providers need a sound message management policy and the infrastructure to support it. They have been slow, however, to adopt data or electronic message retention and retrieval policies. The list of seemingly intractable difficulties includes:

- Shrinking margins for providers
- Unfunded mandates imposed by all levels of government
- Interoperability and privacy concerns
- Changing requirements from regulatory and accrediting bodies.

<sup>1</sup> Redgrave Daley Ragan & Wagner LLP. *Building an ROI Business Case for Email Archiving*. 2006. p. 3.

<sup>2</sup> PriceWaterhouseCoopers. *The Global State of Information Security*. 2007. p. 9.

<sup>3</sup> PriceWaterhouseCoopers. *How healthcare providers are missing opportunities to ensure that investments in security and privacy are also lowering risks*. 2007. p.1.

## Managing Electronic Messaging and E-Discovery for Healthcare Providers

In response to these challenges, providers have adopted either a “save everything” or a “save nothing” approach. While both have the virtue of simplicity, neither is adequate.

Many healthcare providers also mistakenly believe that backup and disaster recovery policies meet their needs. While necessary, backup and disaster recovery are insufficient to meet message retention and retrieval requirements. Data backups only meet the need for recovering lost or damaged files. Locating a particular message or group of messages on a backup or archive tape is a difficult and time-consuming process—and may be impossible if the tape is unreadable. Similarly, responding to a legal discovery order requires a message archive that is indexed, available, and searchable.

E-discovery is a term used to describe the retrieval of electronic stored information in response to a legal proceeding. Federal Rules of Civil Procedure enacted in December 2006 delineate the kinds of materials that are subject to e-discovery, but they do not specify how an organization must meet those requirements. (See the Symantec white paper *2006 Federal Rules of Civil Procedures—E-Discovery and Archiving Impact* for a discussion of the new rules.)

### **Message management and e-discovery challenges**

According to Redgrave Daley Ragan & Wagner, 37 percent of companies use email servers as de facto file systems to store a wide variety of mostly unstructured data.<sup>4</sup> Even more problematic, IT administrators often set a limit on mailbox size (for example, a certain number of megabytes per user), forcing users to discard email to comply with the size limitation. To circumvent these limits, some users create personal email archives (PST or NSF files). Neither solution is optimal: The first one involves the deletion of potentially important messages, and the second is not conducive to locating a particular item.

To be effective and to meet regulatory requirements, a message management system needs to be aligned with a company’s overall policy for retaining and destroying corporate records. For healthcare providers, this most often means that records need to be retained for the periods specified in the HIPAA regulations. For example, HIPAA requires that patient records be maintained for the life of the patient plus six years. This requirement extends to electronically stored records and incorporates the provider’s ability to produce those records in response to a legitimate request.

A strict message management policy is critical in the healthcare industry because patient records are particularly sensitive. According to industry analysts, about 15 to 20 percent of a healthcare provider’s email contains personal health information, the release of which must be carefully managed and documented. The risk of litigation is high because the records often

<sup>4</sup> Op. cit., p. 3.

## Managing Electronic Messaging and E-Discovery for Healthcare Providers

contain diagnosis, treatment, and other information that may reveal the quality of care. For healthcare providers, a crucial component of a message management system is its ability to respond to e-discovery requests with the appropriate information.

While simply storing email messages indefinitely on the email server (the “save everything” approach) may meet regulatory requirements, locating a specific email message or a group of email messages related to a single issue becomes extremely costly. For example, the Boeing Company estimates that every 15 email messages it must find in response to a legal discovery request costs US\$1 million. That is a serious drain on corporate resources, especially since Boeing receives an average of two discovery requests every day.<sup>5</sup> Likewise, if a company does not devise and implement a policy for destroying obsolete records, then the search not only costs more, but it exposes the company to greater risks.

While healthcare providers must permanently store certain information, such as birth and death records, other records can be subject to deletion. In fact, retaining patient records beyond a required time period increases the risk that a discovery request will uncover a document that could undermine the provider’s legal position, when it could have been legally destroyed.

The “save nothing” approach yields equally risky results. Typically, it attempts to circumvent content and retention management requirements by implementing a short (30- to 90-day) message retention period, after which the company routinely destroys the electronic records. (The so-called “safe harbor” provision of the Federal Rules of Civil Procedure does not specify a retention period; it only addresses the effectiveness of a company’s systems in managing the message retention period.) If a plaintiff produces an email trail that the provider fails to corroborate, two outcomes are likely. First, the provider may be unable to defend itself against a claim that may in fact be defensible, and second, the provider may face significant fines for failing to preserve and produce the email.

In a case involving the Washington, D.C., mass transit authority,<sup>6</sup> the authority continued to delete email messages that were more than 60 days old automatically, even after a lawsuit had been filed. The court found the authority’s failure to produce the messages “indefensible” and ordered it to produce backup tapes and to search the tapes for all relevant email. The transit authority was also ordered to pay all the costs of creating and culling the backup tapes.

Failing to preserve or produce email also cost two financial services companies, UBS Warburg and Morgan Stanley, substantial amounts of money: UBS Warburg paid a US\$29 million judgment, and Morgan Stanley was ordered to pay US\$1.758 billion (the amount was later overturned on appeal).<sup>7</sup>

<sup>5</sup> *Ibid.*, p. 6.

<sup>6</sup> *Disability Rights Council of Greater Wash. v. Wash. Metro. Area Transit Auth.*, 2007 WL 1585452 (D.D.C. June 1, 2007).

<sup>7</sup> Kehoe, Jennifer. *Best Practices for Enforcing Legal Holds on E-Mail and Electronic Data through Proactive Archiving*. 2007. pp. 5–6.

### **Identifying best practices**

An established policy for retaining, retrieving, and destroying email and other electronically stored information is the starting point for implementing a message management and archiving system. The primary component of a message management system is an email management program that can accommodate the growing volume of email. The management program should also extend retention and recovery capability to instant messages and shared documents.

An email management program provides secure access through both the corporate email program and a Web-based program that allows access by auditors and other authorized users. The email archive itself tracks access to the archived records, and the IT department can scale up the archive efficiently and securely as the volume of email messages grows.

An effective email management solution also minimizes the risk associated with leaks of confidential personal health information and helps providers defend against internal litigation or human resources complaints, such as wage disputes and harassment claims. Finally, a complete email management and archiving system reduces storage requirements, which decreases the expense and complexity of maintaining storage systems.

A well-designed email archiving program provides hierarchical storage management technology, which retains recent email messages in quickly accessible storage and moves the messages to cheaper, less accessible storage as they age. Another valuable tool in an email archiving program migrates personal data stores (PST and NSF files) to the archive. The complete email management program integrates easily and thoroughly with the company's existing records management program and legacy data.

As instant messages and shared documents become more prevalent, a comprehensive message management system needs to include intelligent archiving for this type of content as well. It may also provide real-time content controls to block IMs that contain restricted information. Another important element is the ability to automatically classify and archive messages on the basis of content and metadata. Automatic classification of messages helps healthcare providers archive only relevant content.

In addition to these capabilities, message management and archiving programs need to incorporate tools to simplify e-discovery requirements. These tools must be able to initiate a litigation hold program as part of an email archiving solution, involving immediate suspension of any planned destruction of documents related to pending or reasonably foreseeable litigation. An effective litigation hold function demonstrates that a healthcare provider is making a good faith effort to comply with e-discovery obligations.

## Developing and implementing a message management and e-discovery program

The first step in developing an effective message management program is to recognize the threat that derives from the absence of such a program. Without effective message management, an organization faces not only increased financial risk, but also greater susceptibility to public relations damage. An efficient message management program serves as an insurance policy against the consequences of the inability to locate a message in response to a legitimate request. Figure 1 illustrates a comprehensive plan for implementing an email management and archiving program.

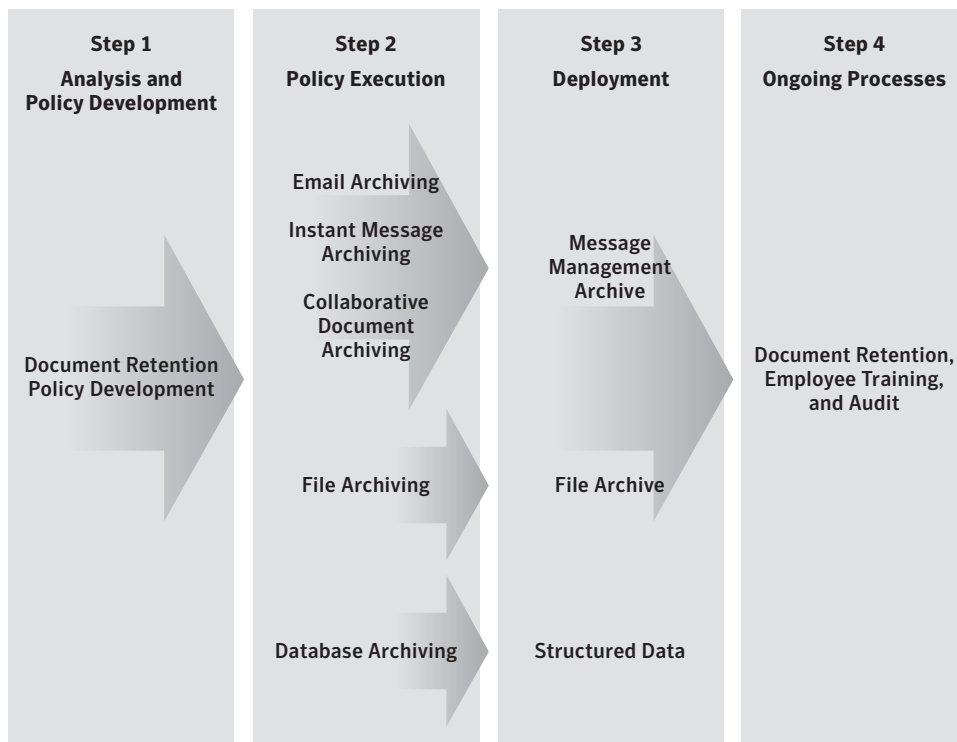


Figure 1. Designing and implementing an email management and archiving program

## Managing Electronic Messaging and E-Discovery for Healthcare Providers

The growth of electronic messaging among healthcare providers requires that they start now to implement a message management system that captures and indexes messages to meet the regulatory requirements of HIPAA, state privacy standards, and the Joint Commission. This section describes the message management system attributes that facilitate message retention and e-discovery.

### **Automatic, secure, and scalable message management**

A high-quality archiving solution automatically captures and indexes all incoming and outgoing messages and attachments so that they can be easily searched and retrieved. Intelligent filtering, retention, and review policies ensure that only relevant content is archived. The solution also offers protection from inadvertent or deliberate deletion of email messages and IMs. Finally, an email management solution is scalable.

### **Efficient archiving**

When an email user attaches a file to a message and sends that message to five users, the email program saves five copies of that message and the attachment. In contrast, an efficient email management system saves only a single instance of the message and its attachment. This de-duplication reduces storage requirements and helps to control storage costs. A message management system that supports hierarchical storage management technology also helps reduce archiving costs.

### **Improved content control**

In response to e-discovery or other information requests, providers are sometimes restricted from releasing personal health information. If the email archiving program cannot differentiate between restricted and releasable information, however, someone must peruse the messages returned by an archive search to determine whether or not a particular item may be released. An email archiving system with granular content control, on the other hand, allows the provider to index messages and documents with a variety of tags, including Bates numbers, social security numbers, account numbers, and medical diagnosis codes, that narrow the parameters of the search and retrieve only those items that meet specific requirements.

## Managing Electronic Messaging and E-Discovery for Healthcare Providers

A robust message management system also permits IT administrators to set policies to block archive access for some users, quarantine certain documents, and establish different policies for incoming and outgoing email. A provider's records retention policy might also include an email journaling requirement, under which all email messages to and from certain individuals are recorded and retained indefinitely.

A fully integrated security program can protect a provider against inbound and outbound security threats from email and IM messages. It helps guard against accidental or deliberate data leakage, enforce compliance with external regulations, and support internal governance procedures. (For more information on creating secure messaging systems, see the Symantec white paper *Critical Infrastructure Security for Healthcare Providers*.)

### **Elimination of personal storage and incorporation of legacy data**

Personal stores of email messages threaten to undermine even the best email retention policy because they can prevent the contents of email messages from being indexed and archived properly. Thus they jeopardize the provider's ability to respond to an e-discovery request. A high-quality email management program automatically converts personal email stores to indexed files that can then be saved according to the organization's retention policy.

Such a program also converts legacy data that may be stored on magnetic tape into usable, indexed files that may be saved and retrieved in accordance with the established retention policy.

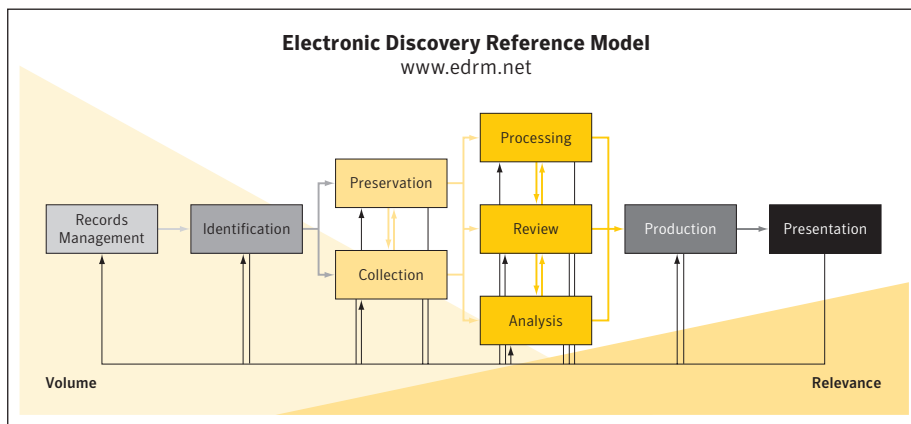
### **Message recovery in native formats**

In response to an e-discovery request, an organization may be required to provide electronic communications in the native (unaltered) format of the original message. The courts have decided that if the parties do not specify or cannot agree on a production format, then electronically stored information must be produced in native format. If the communication was originally an email message, for example, the document produced must also be an email message.

The same holds true for instant messaging and document-sharing applications, which are growing in use among healthcare providers. Instant message usage is growing faster than any other type of electronic messaging system, and 90 percent of healthcare providers have not yet adopted a policy to retain and discover those messages. In fact, many providers attempt to prohibit the use of instant messaging services, which neither solves the problem nor enhances productivity.

## Open approach to e-discovery

E-discovery is a complicated process, often involving multiple internal and external stakeholders using a variety of case management, analytics, and review solutions (see Figure 2). These parties to the e-discovery process typically require access to cases within the archive for review or to litigate the case. An archiving solution must be able to support automated data transfer with chain-of-custody tracking from the archive to complementary e-discovery solutions that service providers or outside counsel may use.



**Figure 2. The Electronic Discovery Reference Model**  
Source: Electronic Discovery Reference Model, EDRM, <http://edrm.net>

## Capability to enforce a litigation hold

When an organization receives a discovery order, it must immediately initiate and enforce a hold on all documents that may potentially be retrieved in response to the order. The organization's normal policy regarding destruction of records must be suspended until further notice. An e-discovery program should provide the capability to enforce multiple litigation holds at one time and to add new content to an existing hold.

## Message management and e-discovery program benefits

The first measure of value for any new software program is the amount of money an organization will save by making the purchase. A message management program reduces costs in three areas: archival storage; administration; and response to discovery, regulatory, or other legitimate inquires.

## Managing Electronic Messaging and E-Discovery for Healthcare Providers

Message management systems that reliably archive a single instance of a message and its attachments can significantly alleviate the demand for storage. Combined with automatic compression, for example, archiving can decrease storage requirements by as much as 50 percent.

Administrative costs also decline because a high-quality email management program reduces requirements for new servers to handle the increasing volume of email at an acceptable level of system performance. For example, a fully functional Microsoft® Exchange server costs about US\$30,000 and often requires additional staff to maintain and operate.<sup>8</sup>

Finally, a high-performing email management program that includes an e-discovery component simplifies retrieving documents in response to a discovery request—at significant cost savings. For example, early in 2007, a person suspected of contracting a particularly virulent strain of tuberculosis flew to Europe to be married and was able to reenter the United States, even though border security agents should have detained him. A news organization in Atlanta filed a request for open records with Fulton County government to receive email messages related to the incident. Fulton County government supports about 7,000 email accounts, and a manual search of the email records would have required weeks or months to complete. Because the county had installed an email management system, it was able to retrieve about 200 relevant email messages in about 90 minutes.<sup>9</sup> Not only did Fulton County circumvent a long and costly search through its email archives, but it also did not experience the negative publicity that would inevitably have followed. Had the request been a legal discovery filing, Fulton County would have accrued financial and accreditation risks if it had failed to produce the messages. Avoidance of those risks surely repaid the cost of implementing the county's email management program.

Maintaining a complete, indexed archive of electronically stored information is critical to comply with a litigation discovery request. With such an archive, the healthcare provider's IT department can collect messages and documents in a centralized location and, more important, find them in a centralized location when the records need to be produced.

E-discovery tools perform three vital tasks that help protect a healthcare provider during the course of litigation. First, they initiate and enforce litigation holds on requested documents and retain and track multiple holds in a single, cohesive system. Second, they permit a provider to quickly and accurately evaluate the merits of a case before meeting with opposing counsel in the required "meet and confer" stage of the new Federal Rules of Civil Procedure. Third, a provider's policy on record retention, maintenance, and deletion are thoroughly documented and enforced, minimizing the risk of penalties.

<sup>8</sup> Alchemy Solutions Group. *Email Archiving, e-Discovery, and Compliance*. 2007. p.15.  
<sup>9</sup> Mullins, Robert. "TB Case Highlights E-Mail Archiving Trend." *InfoWorld*. July 10, 2007.

## Symantec solution for message management and e-discovery

Symantec offers a comprehensive solution that enables healthcare providers to manage risks across the information and messaging lifecycle. Industry-leading message management and e-discovery tools from Symantec lower the total cost of ownership and help providers overcome the challenges of ensuring the security and availability of messaging systems and confidential patient information. The Symantec solution comprises market-leading security and archiving products that help reduce the risk of downtime, control costs, protect confidential information from leakage, and demonstrate compliance with IT policies, internal processes, and external regulations.

### The Symantec solution

Symantec solution	Function	Features and benefits
Symantec Enterprise Vault™	A software-based intelligent archiving platform that stores, manages, and discovers corporate data from email systems, file server environments, instant messaging platforms, and content management and collaboration systems	<ul style="list-style-type: none"> <li>• Automate mailbox management to free users from size restrictions</li> <li>• Optimize storage consumption to minimize costs</li> <li>• Eliminate the need for personal storage files</li> <li>• Implement intelligent archiving to provide insight into archived content</li> </ul>
Automatic Classification Engine	An optional software component that provides intelligent, content-based categorization and tagging of email	<ul style="list-style-type: none"> <li>• Automatically classify and archive email based on content and metadata</li> <li>• Lower storage costs and resources</li> <li>• Archive only relevant content</li> <li>• Enable granular retention</li> <li>• Search and review archive more quickly</li> </ul>
Symantec™ Discovery Accelerator	An optional software module that extends the functionality of Enterprise Vault to enable a powerful and efficient search capability, configure enforcement of litigation holds, and export documents in native formats	<ul style="list-style-type: none"> <li>• Target all internal or external data, including email, files, attachments, and instant messages</li> <li>• Search metadata and full attachments</li> <li>• De-duplicate redundant items</li> <li>• Create multiple databases for scalability, security, and segregation of data</li> <li>• Export to native file system and message formats</li> <li>• Demonstrate due diligence with a full audit trail</li> </ul>

## Managing Electronic Messaging and E-Discovery for Healthcare Providers

### The Symantec solution (continued)

Symantec solution	Function	Features and benefits
Premium Content Control	An add-on subscription service to the Symantec Mail Security 8300 Series appliance that extends the power of standard content filtering to help organizations manage the risks associated with data leakage, regulatory compliance (HIPAA, PCI, and so on), and internal governance	<ul style="list-style-type: none"> <li>• Easily set up content-based policy actions for delivery or nondelivery, email encryption, archiving, and incident management</li> <li>• Quickly deploy policies to address regulatory compliance and internal governance requirements</li> <li>• Identify and block confidential patient information</li> </ul>
Symantec IM Manager	An optional software module that seamlessly manages, secures, logs, and archives corporate instant messaging traffic; IM Manager provides certified support for public and enterprise IM networks, including granular policy enforcement and security controls for files, audio, video, VoIP, application sharing, and other real-time communication capabilities	<ul style="list-style-type: none"> <li>• Block and manage IM use on public and enterprise networks</li> <li>• Support archiving and discovery of IM communications</li> <li>• Provide real-time content controls to block messages containing restricted words or phrases</li> <li>• Simplify the e-discovery process</li> <li>• Provide a complete picture of IM and email communications</li> </ul>

### Conclusion

An effective solution to message management and e-discovery regulations couples a healthcare provider's business processes with technology-based solutions that can substantially reduce a provider's costs and risks. A solution that incorporates e-discovery functionality with a message management program enables a healthcare provider to locate, review, and produce relevant medical records without jeopardizing patient privacy.

An effective solution should include the following:

- A message management system must be automatic, secure, and scalable
- An email archiving program should use storage resources efficiently
- An email archiving program needs to provide robust content control
- An email archive needs to eliminate the need for personal storage and incorporates legacy data
- A message retrieval system has to support recovery in native formats
- An archiving program has to support an open approach to e-discovery
- An e-discovery program has to be able to initiate and enforce multiple litigation holds

## About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world.

The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries.

More information is available at [www.symantec.com](http://www.symantec.com).

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation  
World Headquarters  
20330 Stevens Creek Boulevard  
Cupertino, CA 95014 USA  
+1 (408) 517 8000  
1 (800) 721 3934  
[www.symantec.com](http://www.symantec.com)

Copyright © 2007 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and Enterprise Vault are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Microsoft is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries. Other names may be trademarks of their respective owners. Printed in the U.S.A. 11/07 13518082