MessageSolution™

Enterprise Archiving, eDiscovery, Migration

HIPAA Compliance:

The Health Insurance Portability and Accountability Act (HIPAA)

MessageSolution Enterprise Email Archive 6.0 for the Healthcare Industry

Disclaimer: *This document is not a comprehensive or legally permissible guide to HIPAA compliance. Organizations should NOT rely on this overview in place of professional legal advice. While the MessageSolution Platform will not ensure compliance on its own, it is a valuable tool for efficiently and cost effectively managing electronic protected health information (ePHI).*

Regulatory Compliance:

The Health Insurance Portability and Accountability Act (HIPAA)

MessageSolution Enterprise Email Archive 6.0 for the Healthcare Industry

Table of Contents

Introduction

While regulatory compliance is a common concern for several industries, the Health Insurance Portability and Accountability Act (HIPAA) in particular, affects hundreds of thousands of organizations with potentially severe consequences for both privacy breach victims and the institution itself.

According to an independent survey by the Ponemon Institute, the healthcare industry loses around $7 billion a year due to HIPAA data breaches and at least 94% of healthcare organizations have had at least one data breach in the last two years. 45% (almost half) reported more than 5 data breaches in those 2 years! Since 2010, the average economic impact of a data breach increased from $400,000 to a total of $2.4 million for those 2 years.

While some breaches are more benign than others, the study found that 42% of data breaches can be traced back to employee mistakes or unintentional actions. Due to improperly safeguarded data in healthcare institutions, thousands of patients and providers are potentially compromised yearly. This opens doors for expensive litigation and other legal repercussions.

MessageSolution provides an efficient solution that allows each organization to customize email, SharePoint and file system archiving, retention and privacy policies to help maintain HIPAA compliance. Configure Archive Access, Audit Control, Retention Management, Data Integrity Assurance, Data Transmission Security, eDiscovery, and Litigation Support, etc. The MessageSolution Platform allows organizations to balance record retention and other HIPAA compliance measures with data storage optimization, mitigating unnecessary legal risk.

The healthcare industry loses around

$7 billion

a year due to HIPAA data breaches

$2.4 Million

The average economic impact of one data breach over 2 years

94%

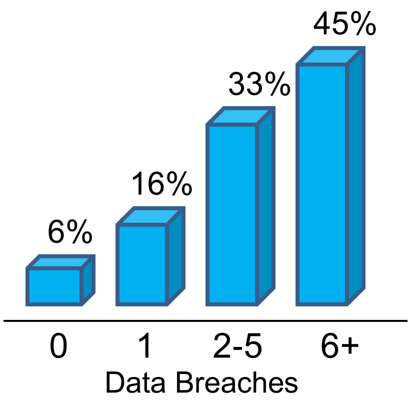
The percentage of organizations that had at least 1 data breach in the past 2 years

45%

The percentage of organizations that had at over 5 data breaches in the past 2 years

Number of Reported HIPAA Data Breaches Over 2 Years

Data taken from 2012 Ponemon Institue Study



What is HIPAA?

Enacted in 1996, the Health Insurance Portability and Accountability Act (HIPAA) addresses the transferability of health insurance and the privacy and accessibility of patient information. HIPAA consists of two titles. Title I protects health insurance coverage for workers and their families when they change or lose their jobs. Title II, also known as the Administrative Simplification Provisions, requires national identifiers for providers, health insurance plans, employers, etc. and put in place the national standards for the handling of relevant electronic information. The Administrative Simplification Provisions also address the security and privacy of medical (patient) data.

In response to HIPAA, the US Department for Health and Human Services (HHS) published three rules:

The Privacy Rule

The Standards for Privacy of Individually Identifiable Health Information, or Privacy Rule, establishes national standards for the use and disclosure of individuals' electronic protected health information (ePHI).

The Security Rule

The Security Standards for the Protection of Electronic Protected Health Information, known widely as the Security Rule, addresses the technical and procedural safeguards that must be put in place to secure ePHI.

The Omnibus Rule

Recently announced in January 2013, the Omnibus Rule implements several provisions from the 2010 Health Information Technology for Economic and Clinical Health Act (HITECH Act). It establishes stronger procedures for the deletion of ePHI following patients' death and harsher penalties for privacy violations.

Find more information about HIPAA Information at the website for the US Department for Health & Human Services (HSS): http://www.hhs.gov/ocr/privacy/index.html

To Whom Does it Apply?

HIPAA rules to all health plans, health care clearinghouses, and to any health care provider who transmits any ePHI to which HIPAA applies (private practices, hospitals, outpatient facilities, etc.). They also apply to “business associates.” A “business associate” is a person or entity that performs functions as a third-party to organizations or activities that involve the use or disclosure of ePHI from covered entities. (45 CFR 160.103).

Examples of HIPAA Business Associates.

- A CPA firm whose accounting services to a health care provider involve access to protected health information.
- An attorney whose legal services to a health plan involve access to protected health information.
- An independent medical transcriptionist that provides transcription services to a physician.
- A pharmacy benefits manager that manages a health plan’s pharmacist network.

What Can Go Wrong?

In the last three years alone, there have been over 70,000 HIPAA violation complaints. According to the HIPAA & Breach Enforcement Statistics for September 2013, the privacy areas investigated most often were:

- Impermissible uses and disclosures of protected health information (PHI)
- Lack of PHI safeguards
- Lack of patient access to their PHI
- Uses or disclosures of more than the Minimum Necessary PHI
- Lack of administrative safeguards of electronic PHI

Before the HITECH Act and Omnibus Rule were established, the maximum penalty per year per violation was $25,000. Now it’s the maximum fine is $1.5M and anywhere from one to ten years in prison depending on the maliciousness of the violation.

Just this past January, The Hospice of North Idaho (HONI) has agreed to pay $50,000 to settle potential HIPAA violations stemming from the theft of an unencrypted laptop. In July, one organization which serves nearly 36 million people through its affiliated health plans, agreed to pay $1.7M for potential violations of the HIPAA privacy and security rules. HHS claimed that access to personal data for 600K+ people (including names, dates of birth, addresses, Social Security numbers, telephone numbers and health information) was made available to unauthorized users as the result of online security weaknesses.

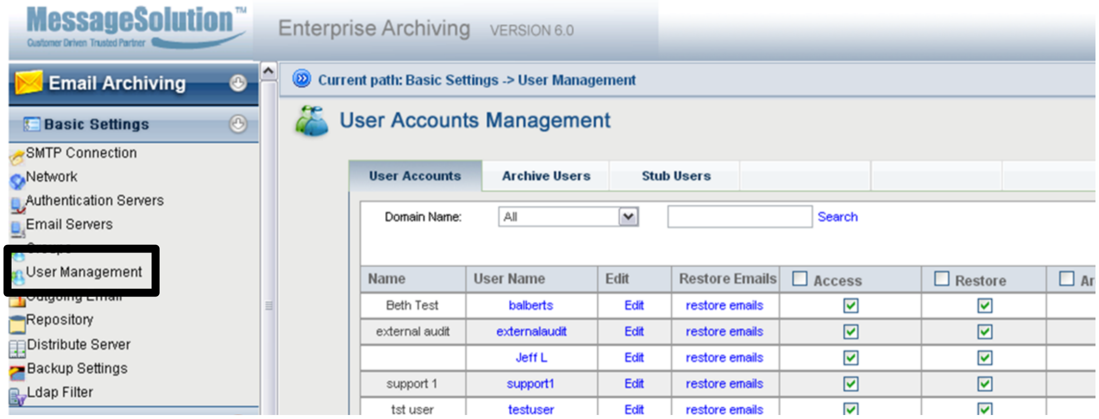
How Can Email Archiving Help?

While HIPAA does not specifically require email archiving, it does mandate that certain types of documentation be retained and protected. These include policy or procedural documentation (including notices of privacy practices, consents, authorizations and other standard forms, etc.), patient requests, complaints and training material. Email archiving can be a powerful tool for efficient and cost effective HIPAA compliance management. MessageSolution Enterprise Email Archive (EEA) helps organizations achieve and maintain HIPAA compliance in the following ways:

1. Administrative Safeguards

The Privacy Rule standard limits disclosures of ePHI to the "minimum necessary." The Security Rule requires authorized, policy-based access to all ePHI.

MessageSolution EEA delivers strict Information Access Management. The system administrator can enact policy-based archive access. Multi-tiered access permissions can are enabled for individual users or user groups based on elements such as department or clearance level. Features like archive access, archiving functionality and data restoring capabilities can all be independently enabled for each user or user group.



Current path: Basic Settings -> User Management

User Accounts Management

Domain Name: All

Name	User Name	Edit	Restore Emails	☐ Access	☐ Restore	☐ Ar
Beth Test	balberts	Edit	restore emails	☑	☑	
external audit	externalaudit	Edit	restore emails	☑	☑	
	Jeff L	Edit	restore emails	☑	☑	
support 1	support1	Edit	restore emails	☑	☑	
tst user	testuser	Edit	restore emails	☑	☑	

MessageSolution Enterprise Email Archive (EEA) 6.0
Administrator Console – User Management Menu

EEA fully integrates with email client directory services (like Active Directory, Domino Directory, GroupWise eDirectory, etc). Among other benefits, this allows the system administrator to import all users/user groups directly from the email directory service. Possible email archive access capabilities include:

Administrator(s): Unlimited access capabilities, Auditor/Legal configuration access, delete capabilities

User(s): Search, retrieve, restore, and configurable delete capabilities for their personal archive and for designated custodian archives

2. Physical Safeguards

The Security Rule also affects physical data security, facility access and control. A covered entity must limit physical access to its facilities while ensuring that authorized access is allowed. With MessageSolution, archived data is stored on archiving servers located on-site with the HIPAA-compliance organization or in the MessageSolution Cloud. All MessageSolution data centers are SSAE Type II certified with security entry (biometrics, key, and password), UPS & diesel power generators (with emergency contracts), temperature controller (designated hot/cold isles on raised floors), and state of the art fire suppression, etc.

3. Technical Safeguards

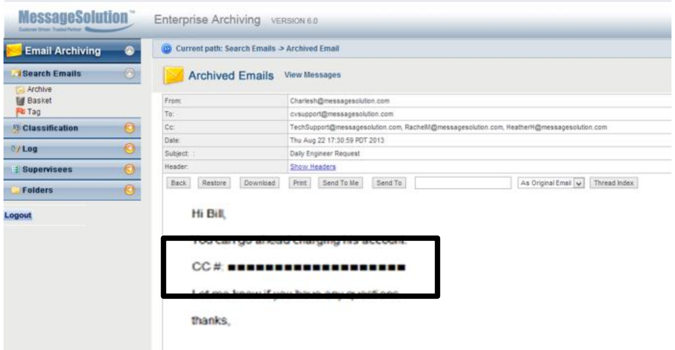
The HIPAA Security Rule sets strict technical standards as well.

- Access Control

A covered entity must implement technical policies and procedures that allow only authorized persons to access ePHI.

As mentioned above, MessageSolution EEA delivers granular, policy-based archive access. With proper policies in place, this helps ensure that sensitive data is not access by unauthorized users.

MessageSolution is one of the few vendors to offer configurable **Data Redaction** to further ensure privacy. Configure redaction policies for patient IDs, Social Security numbers, etc.



From: Charlesh@messagesolution.com
To: cvsupport@messagesolution.com
Cc: TechSupport@messagesolution.com, RachelM@messagesolution.com, HeatherH@messagesolution.com
Date: Thu Aug 22 17:30:59 PDT 2013
Subject: Daily Engineer Request
Header: Show Headers

Hi Bill,

You can go ahead charging his account.

CC #: [redacted]

Let me know if you have any questions

thanks,

MessageSolution Enterprise Email Archive 6.0
Data Redaction

- Audit Controls

A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use ePHI. MessageSolution EEA helps organizations maintain audit controls in several ways. Enterprise Email Archive tracks archiving processes and user activity within the archive by maintaining multiple logs and reports. These track archive use, data access, etc. and preserves the chain-of-custody of email data. Reports can be exported and used in combination with other reports and reporting tools as part of compliance governance, litigation support or performance tuning.

MessageSolution Reports and Logs Include:

Search Log -- details who searched and when; terms used to search; number of queries returned

Access Log -- monitors who accessed the archive, what action was taken; actions include view, download, restore, log in, etc.

Archiving Report -- which email boxes are being archived; how many messages are in the email box; size user is occupying in archive storage repository

Status Reports -- reflect the current state of the archiving application and system status. User, actions, IP addresses, subject, sender, and inquiries are some of the information available from the reports, which help provide a picture of the type of usage the archive is put to

Customizable Reports -- can also be configured to report on specific senders, recipients and content keywords

Temporary and limited access can be granted to third-party auditors and legal counsel. With **Auditor/Legal Access**, auditors or attorneys will be able to independently search and access selected custodians' mailboxes.

When an audit is performed, random sampling is typically used in lieu of overseeing every piece of archived mail. With MessageSolution **Random Sampling** feature, auditors can set granular parameters for the sample. Random sampling is used to monitor regulatory compliance.

- Retention Management

A covered entity must ensure that HIPAA-compliant data is retained for six (6) years while the individual is living and no more than fifty (50) years after an individual is deceased. MessageSolution provides **policy-based retention management**. The system administrator can granularly configure simultaneously active retention policies based on users, user groups, etc. Data applicable to more than one retention policy adheres to more conservative policies.

- Integrity Controls

A covered entity must implement policies and procedures to ensure that ePHI is not improperly altered or destroyed. MessageSolution Enterprise Email Archive delivers safeguards to ensure that ePHI is not prematurely destroyed. Hash code technology also ensures the integrity of all archived data.

- Transmission Security

A covered entity must implement technical security measures that guard against unauthorized access to ePHI that is being transmitted over an electronic network. MessageSolution offers options for both **SSL and AES Encryption** to protect stationary data and data in transit for cloud archiving and eDiscovery.

- Business Associates Agreement (BAA)

When a covered entity uses a contractor or other non-workforce member to perform "business associate" services or activities, the Rule requires that the covered entity include certain protections for the information in a Business Associate Agreement. The agreement must impose specified written safeguards on all ePHI used or disclosed by its business associates. MessageSolution regularly provides BAAs to HIPAA-compliant organizations. Signed by MessageSolution’s Head of Operations, the agreement explicitly outlines MessageSolution’s potential exposure and handling of all ePHI.

MessageSolution Enterprise Email Archiving

MessageSolution Enterprise Email Archive (EEA) is a one-stop solution for compliance archiving, eDiscovery and storage management. It provides a secure, highly interactive data store and high-performance eDiscovery system for corporate email systems. EEA drastically reduces the cost and eliminates complications associated with data storage, recovery and information archiving. Available as on-premise, hosted and solutions, MessageSolution technologies also give users controlled and self-serving access to archived data.

MessageSolution EEA collects, replicates, compresses and indexes all data for advanced searching, eDiscovery and compliance management. Archived data is almost immediately available for retrieval for business-critical situations, audits or eDiscovery requests. In addition to archiving the contents of email messages, EEA transparently captures, indexes and archives all compliance-related metadata, messages, attachments, contacts and calendar items without impacting end-users.

MessageSolution Enterprise Email Archive supports most corporate email environments including Microsoft Exchange 5.5-2013 and Office 365, IBM Lotus Domino 6.5-8.5, Novell GroupWise 7.0-2012, GMAIL and Linux/UNIX-based email servers.

In addition to regulatory compliance management, the MessageSolution Platform also offers advanced functionality healthcare organizations:

eDiscovery, Litigation Support

Unfortunately, the healthcare industry is notoriously litigious. MessageSolution ensures eDiscovery-readiness by indexing all archived data for searchability. eDiscovery functionality includes high-performance searching for comprehensive eDiscovery results, legal hold, data redaction, bates numbering, etc.

Email Restoration, Intelligence Management

Permitted users can restore archived email back onto the email server in cases of accidental or malicious deletion.

Solution Adaptability

Granular configuration control and flexible solution architecture ensure that organizations have the ability to easily adapt to all new standards or rules.

HIPAA Compliance in the Cloud

MessageSolution also supports HIPAA-compliant cloud archiving and eDiscovery Cloud Services. With the same features and functionality of the on-premise solution, MessageSolution cloud archiving and eDiscovery cloud services are a viable alternative to traditional on-premise archiving.

All MessageSolution Data centers are bi-annually audited to maintain their SSAE Type II certification status. Data center security measure include biometrics, key, and password security. All data centers will include UPS, diesel power generators (with emergency contracts), temperature controller (designated hot/cold isles on raised floors), and state of the art fire suppression equipment with an N+1 minimum design for the facility, etc. There are also options for SSL and AES encryption.

In addition to the MessageSolution cloud network, EEA also fully integrates with Microsoft Azure, IBM SmartCloud, Savvisdirect, Amazon EC2, OpSournce, etc. for public cloud storage or disaster recovery options.

Avoid Paying Millions for HIPAA Breaches or Retroactive eDiscovery

With the increased adoption of electronic communications and records in the healthcare industry, HIPAA compliance is an extremely critical and an extremely multi-faceted complication with expensive consequences for lackluster or non-compliance. MessageSolution archiving and eDiscovery solutions help organizations achieve and maintains HIPAA Compliance with on-premise, hosted and cloud-based solutions for all size organizations. Assuming a healthcare organization has at least one HIPAA breach a year (as 94% of them did according to the Ponemon Institute), MessageSolution will help organizations economic impacts of over $2.4 Million in the short term and $17 Million+ in the long term. Technically, HIPAA violations can also be punished with anywhere from one to ten years in prison.

MessageSolution Enterprise Email Archive also serves as a preemptive eDiscovery solution. In general, archiving solutions provide the perfect platform for an end-to-end eDiscovery process. All the data is already ingested into a centralized data store and heavily indexed for searchability. Retroactive solutions extremely expensive and ingesting large amounts of data can take months. According to Ben Kerschberg, a contributor at Forbes.com in his article about the cost of eDiscovery, most eDiscovery vendors typically charge by a per-gigabyte model. Considering the amount of ESI in question with most healthcare providers, this can be exceptionally expensive. A study by the Minnesota Journal of Law, Science and Technology estimates that eDiscovery costs range anywhere from $5,000 to $30,000 per gigabyte and The Rand Corporation study references claims that the total costs per gigabyte reviewed were generally around $18,000.

The MessageSolution eDiscovery workflow in particular, outsources all eDiscovery data requests from IT directly to the legal department. They can quickly locate and collect all relevant data for review. Reviewers can then tag, annotate and publish data as needed. This saves hours of billable time.

Tangible Cost Savings
With MessageSolution Enterprise Email Archive

Due to a high in-process data compression rate, Single Instance Storage and de-duplication, Enterprise Email Archive can save up to 75% of archiving server storage requirements. MessageSolution leverages this for industry-leading scalability and can archiving for over 25,000 users on one archiving server. Other on-premise archiving solutions require 4-8 servers for the same user-base. High scalability also make the solution easy to run on a virtualized server. Depending on the quality of the archiving server, MessageSolution saves organizations roughly $3,000-5,000 per server (although it can easily be more.) MessageSolution can also completely eliminate hardware requirements with their secure, compliant archiving and eDiscovery cloud services.

Many other archiving solutions also require SQL database licensing. This can easily double the cost of the archiving servers depending on the size of the database. In addition to initial database system licensing, annual support is sometimes required. SQL databases are also licensed on a per-core basis. Most databases have anywhere from 4-8 cores. SQL licensing can easily cost around $26,000-$54,000 with around 20% annual maintenance per year. Enterprise Email Archive does not require SQL licensing or any other third-party software. Instead of relying on SQL database (designed for structured data), the MessageSolution platform leverages an embedded database designed specifically for unstructured data like most email content.

About MessageSolution, Inc.

MessageSolution, an industry leader in enterprise-class information archiving and eDiscovery solutions, provides advanced, policy-based archiving and legal eDiscovery capabilities for email, SharePoint and file system environments. Available for on-premise, Cloud-based or MSP-hosted environments, MessageSolution Information Archive and eDiscovery Platform enforces regulatory compliance, regulated data management and high data accessibility to ensure eDiscovery-readiness at all times. A high, in-process compression rate coupled with Single Instance Storage allows MessageSolution to save up to 75% of storage space and archive for 25,000+ users on one single server. Leveraging full email client integration, MessageSolution offers a seamless solution for searching and accessing archived data. The MessageSolution Platform is intuitive and user-friendly, making it easy for users at all company levels to utilize.

MessageSolution has an intricate network of clients, Enterprise Information Archive Solution Resellers, Advanced Managed Service Providers and Elite Premium Alliance Partners all across the world. Organizations from all industries, including multiple levels of government, healthcare providers, law firms and even a professional football team, leverage our unique software and dedicated services to manage their archiving and eDiscovery needs.

MessageSolution is headquartered in Milpitas, California, in the heart of Silicon Valley, with additional offices in Castro Valley, California, and Beijing, China. MessageSolution maintains operations in North America, Europe, and Mainland China, along with distribution channels established in North America, Europe, Australia, Africa, and Asia Pacific.

External Sources

“Accounting for the Costs of Electronic Discovery” David Degnan, Minnesota Journal of Law, Science & Technology <http://mjlst.umn.edu/prod/groups/ahc/@pub/@ahc/@mjlst/documents/asset/ahc_asset_366139.pdf>

"Health Information Privacy." US Department of Health and Human Services. <http://www.hhs.gov/ocr/privacy/index.html>

“HHS announces first HIPAA breach settlement involving less than 500 patients - Hospice of North Idaho settles HIPAA security case for $50,000” Jan. 2, 2013 <http://www.hhs.gov/news/press/2013pres/01/20130102a.html>

"HIPAA Rules, Outdated Tech Cost U.S. Hospitals $8.3B a Year." *Computerworld*. <http://www.computerworld.com/s/article/9238954/HIPAA_rules_outdated_tech_cost_U.S._hospitals_8.3B_a_year>.

“HIPAA Administrative Simplification” Regulation Text
45 CFR Parts 160, 162, and 164 (Unofficial Version, as amended through March 26, 2013)
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf>

“The Demise of Electronic Discovery’s Per Gigabyte Price Model” Ben Kerschberg, a Forbes.com Contributor <http://www.forbes.com/sites/benkerschberg/2011/09/13/the-demise-of-electronic-discoverys-per-gigabyte-price-model/>

“Third Annual Benchmark Study on Patient Privacy & Data Security” Ponemon Institute LLC. December 2012. <http://www2.idexpertscorp.com/assets/uploads/ponemon2012/Third_Annual_Study_on_Patient_Privacy_FINAL.pdf>

"WellPoint to Pay $1.7 Million HIPAA Penalty” Modern Healthcare. <http://www.modernhealthcare.com/article/20130711/NEWS/307119954>.

“Where the Money Goes” The Rand Corporation <http://www.rand.org/pubs/monographs/MG1208.html>