

HIPAA and Beyond: An Update on Healthcare Security Regulations for Email



Healthcare regulations for IT security are now broader than ever—covering not just HCOs but their business partners, as well. All kinds of companies, from Web hosting firms to accountants, are now subject to HIPAA security regulations and other data privacy regulations, if they have HCOs as customers or partners. Meanwhile, the penalties for botching data security and allowing a breach to occur are increasingly onerous. Fines are bigger, notification requirements are more stringent and enforcement organizations have new incentives for taking action.

If you manage IT assets or operations for a U.S. healthcare organization or for the business partner of a U.S. healthcare organization, this paper provides a quick overview of what you need to know about the latest security and data breach regulations for the healthcare industry. It also outlines what to look for in a secure email solution for complying with the web of regulations that now apply to so many companies.

Contents

- Introduction.....1**
- Let’s Start with HIPAA1**
 - The EDI Rule.....2
 - The Privacy Rule.....2
 - The Security Rule2
- Penalties and Patterns of Enforcement3**
 - New HIPAA Regulations Included in ARRA.....3
- Other Data Breach Notification Laws.....5**
 - The FTC’s Data Breach Notification Law5
 - Another HHS Data Breach Notification Law6
 - Other Relevant Data Privacy Laws.....6
- Where Does This Leave Enterprises in the Healthcare Industry?7**
- Requirements for Secure Email7**
 - Smart Detection of PHI7
 - Standard and Custom Dictionaries for Private Data8
 - Rigorous Encryption.....8
 - Flexible Deployment Scenarios.....8
 - Archiving Capabilities to Comply with Record Retention Requirements9
 - Requirements Summary.....10
- Conclusion10**
- For Further Reading11**
- About Proofpoint, Inc.12**

Introduction

Social networks, blogs, and Twitter might be getting all the press these days, but email remains the most important communications channel for business. Email even surpasses the telephone in frequency of use, according to a 2009 study by Osterman Research.¹

Email is popular throughout the healthcare industry, among providers, insurers, and others. The industry's slow but steady transition from paper-based records to electronic medical records (EMR) promises to only increase the importance of email and other forms of online communication. When health records and customer account records are electronic, it makes sense to transfer them by email or a file transfer protocol such as FTP, rather than U.S. mail or fax, as long as such transmissions are properly secured.

Email is popular because it's convenient and efficient. But it's risky, too. Traveling over the Internet, an unencrypted email message is about as secure as words written on the back of a postcard. The message can be intercepted and read at any of its many hops across servers between sender and receiver. If the message contains confidential information, such as Social Security numbers or health records, the privacy of that information is in jeopardy.

Enterprises in all industries, including healthcare, know they need to do something about email security. They need to protect the good messages—including messages that contain private data—while blocking the bad messages, such as spam.

Most IT executives and engineers in healthcare organizations (HCOs) are aware of government-mandated regulations for encrypting confidential email. The best known regulations are those set forth in the Healthcare Information Portability and Accountability Act (HIPAA) of 1996, which established standards for exchanging healthcare information and ordered HCOs (which the HIPAA regulations refer to as “covered entities” or CEs) to encrypt email containing confidential patient data.

What these executives and engineers might not know is that the recently passed stimulus bill, the American Recovery and Reinvestment Act (ARRA) of 2009, includes new, stiffer regulations for protecting patient data in email. And states such as Nevada and Massachusetts have recently passed their own laws for data security and data breach notifications that affect any HCO with patients in those states.

Healthcare regulations for IT security are now broader than ever—covering not just HCOs but their business partners, as well. All kinds of companies, from Web hosting firms to accountants, are now subject to HIPAA security regulations and other data privacy regulations, if they have HCOs as customers or partners. Meanwhile, the penalties for botching data security and allowing a breach to occur are increasingly onerous. Fines are bigger, notification requirements are more stringent and enforcement organizations have new incentives for taking action.

If you manage IT assets or operations for a U.S. healthcare organization or for the business partner of a U.S. healthcare organization, this paper provides a quick overview of what you need to know about the latest security and data breach regulations for the healthcare industry. It also outlines what to look for in a secure email solution for complying with the web of regulations that now apply to so many companies.

Let's Start with HIPAA

HIPAA was passed by the U.S. Congress and signed by President Clinton in 1996. One of the bill's original goals was to make it easier for workers to continue their healthcare insurance coverage, even for pre-existing conditions, when changing jobs. To ensure uninterrupted coverage for patients, HCOs need to be able to pass patient records and other data back and forth. For this to happen efficiently and reliably, healthcare records would need to become more portable (hence the ‘Portability’ in the act's title), so the bill set forth new terminology and Electronic Data Interchange (EDI) code sets for transmitting data. Of course, transferring confidential health records is risky; private data might inadvertently be exposed to inappropriate or even malicious parties. So HIPAA legislators also set forth security mandates that came to address data security and privacy issues at large in healthcare.

¹ See *The Critical Need for Encrypted Email and Secure File Transfer Technologies*, Osterman Research, July 2009.

Before HIPAA, security measures for patient data varied from state to state and from one health-care organization to another. Once enacted, HIPAA provided the U.S. healthcare industry with uniform, nationwide guidelines that emphasized both data security and data portability.² For most HCOs, the HIPAA Privacy Rule went into effect on April 14, 2003. By now, it applies to all HCOs in the U.S.

From the point of view of IT executives and administrators, three parts of HIPAA merit special attention:

- **The EDI Rule (162.1000):** which establishes standard health information terminology and electronic code sets
- **The Security Rule (164.306):** which establishes safeguards to protect the confidentiality, integrity, and availability of electronic protected health information (PHI)
- **The Privacy Rule (164.502):** which orders HCOs to protect PHI and defines the allowable uses and disclosures of PHI, in contrast to “de-identified” health information³

The EDI Rule

The EDI Rule defines classification systems and other code sets that HCOs should use in healthcare records. For example, the EDI Rule mandates that HCOs use the *International Classification of Diseases, 9th Edition, Clinical Modification, Volumes 1 and 2*, when describing diseases, injuries, impairments, and their causes.

Standardizing healthcare terminology eliminates confusion among providers and insurers. It also helps IT departments detect information that could require special treatment to comply with the Security Rule or the Privacy Rule.

The Privacy Rule

The HIPAA Privacy Rule states that HCOs must protect the privacy of patient data. They must “reasonably safeguard” patient data from intentional or unintentional use or disclosure, except as necessary for legitimate medical or business reasons. HCOs must train employees on policies and procedures for protecting patient data.

Protected health information (PHI) is any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment.⁴ PHI includes not only a patient’s name, address, phone number, and Social Security Number (SSN), but also dates (such as hospital admittance and discharge dates), and health plan beneficiary numbers.⁵

The Security Rule

The HIPAA Security Rule requires HCOs to protect the confidentiality, integrity, and availability of the PHI they “create, receive, maintain, or transmit.” HCOs should protect against “any reasonably anticipated threats or hazards” to this data. To protect PHI, whether it’s being stored on a server or transmitted over a network, HCO’s must put in place security policies and practices related to:

- Access control
- Audit controls
- Authentication
- Transmission security

On the subject of Technical Safeguards, HIPAA requires HCOs to “implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.”

2 <http://www.hipaaps.com/main/background.html>

3 “De-identified” information is information that excludes any details, such as a complete Social Security Number, that could be used to identify a specific person.

4 <http://cphs.berkeley.edu/content/hipaa/hipaa18.htm>

5 http://privacyruleandresearch.nih.gov/research_repositories.asp

Penalties and Patterns of Enforcement

The penalties for violating HIPAA's security rule are steep. An individual who discloses PHI may be fined up to \$50,000 and be sentenced to 1 year in jail. If the individual committed the disclosure under false pretenses, the fines can reach up to \$100,000 and the jail time can extend to 5 years. If the individual intended to sell or use the information for personal gain or malicious harm, the penalties become steeper yet: up to \$500,000 in fines and up to 10 years in jail.

Between April 2003, when the first mandates took effect, and January 2008, more than 31,000 HIPAA violations were reported to the U.S. Department of Health and Human Services (H.H.S.). Upon investigation, about two thirds of these violations were dismissed as not being true violations of HIPAA. About 8,000 cases were closed without any significant penalties being assessed. Throughout this period lasting nearly five years, no company was penalized with a fine, and no company official was jailed.⁶ Despite all the admonitory pronouncements of legislators, law firms, and analysts, it seemed as though HIPAA investigators were going to continue taking a friendly—even complacent—approach toward working with HCOs about HIPAA violations.

Then an investigation by the Federal Trade Commission (FTC) determined that pharmaceutical giant CVS Caremark had violated HIPAA's security and privacy rules. In 2006, CVS employees discarded pill bottles labeled with patient names, medication instruction sheets, and computerized prescription orders in open trash containers. The FTC deemed these actions a violation of HIPAA, and, in February 2009, levied a \$2.25 million fine against CVS. (For its part, CVS denied any wrongdoing, but agreed to settle the case.)⁷

The CVS case marked a turning point in HIPAA enforcement. Through the multi-million dollar penalty levied against CVS, the federal government seemed to be signaling to the industry that, after years of taking a primarily consultative approach, investigators were prepared to get tough about enforcing HIPAA privacy and security regulations.

As if the CVS example weren't worrisome enough for healthcare IT workers, new HIPAA regulations in the 2009 economic stimulus bill broaden the coverage of HIPAA and provide strong incentives for investigators to uncover violations and to assess heavy fines. An understanding of these new provisions is essential for any organization hoping to achieve HIPAA compliance today.

New HIPAA Regulations Included in ARRA

Best known for its allocation of \$787 million to stimulate the U.S. economy, the American Recovery and Reinvestment Act of 2009 (ARRA) includes new legislation that broadens the scope of HIPAA and gives HIPAA investigators direct, monetary incentive for pursuing violators. The HIPAA-specific parts of ARRA are found in the Health Information Technology for Economic and Clinical Health Act (HITECH), which Congress included in the overall ARRA legislation.

Broadening the Scope of HIPAA Coverage

HITECH broadens the scope of HIPAA to cover all business associates of HCOs. This means that any accounting firm, legal firm, IT consultancy, or other business partner of an HCO must comply with HIPAA security mandates to protect PHI. Once the new HITECH provisions for business associates take effect in February 2010, these organizations will face the same civil and legal penalties that doctors, hospitals, and insurance companies face for violating the HIPAA Privacy Rule.

Penalties that Provide an Incentive for Enforcement

To encourage enforcement of the HIPAA regulations, HITECH calls for HIPAA civil penalties to be paid directly to the U.S. Department of Health and Human Services' Office of Civil Rights Enforcement. Now those responsible for enforcing HIPAA regulations benefit directly from any fines they levy against violators. This arrangement gives HHS investigators a strong motivation

6 "HIPAA: Clean bill of health, or dying a slow death?", Paul Korzeniowski, SearchFinancial-Security.com, http://searchfinancialsecurity.techtarget.com/news/article/0,289142,sid185_gci1294167,00.html

7 "CVS to pay \$2.25 million to settle HIPAA violation," Dan Kaplan, SC Magazine, February 18, 2009, <http://www.scmagazineus.com/CVS-to-pay-225-million-to-settle-HIPAA-violation/article/127570/>

How Often is PHI Found in Outbound Email?

In its sixth-annual survey on outbound email and data loss prevention issues, Proofpoint found that more than one-third (34%) of large organizations investigated a suspected violation of privacy or data protection regulations via email.

In addition, more than one quarter (26.5%) of companies said that it is "common" or "very common" to find personal healthcare, financial or identity data that may violate privacy and data protection regulations in email leaving their organizations.

Despite these risks, only 35.5% of responding companies said that they had deployed technology that can detect PHI in outbound email.

More statistics about outbound email and data loss can be found in the full report, available from:

www.proofpoint.com/outbound

to make fines as large as possible, since the proceeds go directly into their own coffers. If an enterprise was hoping that the HHS might return to its earlier live-and-let-live attitude toward HIPAA compliance, this new enforcement model suggests that hope is seriously misplaced.

HITECH not only changes how fines will be levied, it also raises the upper limit on the fines that can be imposed. An HCO or business partner who violates HIPAA may have to pay fines reaching as high as \$1.5 million per calendar year. In addition, private citizens and lawyers can now sue to collect fines for security breaches. Overall, HITECH considerably increases the potential financial liability of any organization that mishandles the PHI that passes through its IT infrastructure.

Data Breach Notification Rules

The HITECH Act also includes new data breach notification rules that apply to HCOs and business partners. If an employee discovers a PHI security breach, the employee's organization has only 60 days in which to notify each individual whose privacy has been compromised. If the organization is unable to contact ten or more of the affected individuals, it must either report the security breach on its Web site or issue a press release about the breach to broadcast and print media. If the breach affects 500 or more individuals, the organization must additionally notify the Security of the HHS, along with major media outlets. The HHS will then report the breach on its own Web site.⁸

Clearly, the days of the HHS quietly working with HCOs to correct disclosure problems are over. HIPAA security violations are about to become more public.

How consumers react to an increasing amount of news about healthcare security breaches remains to be seen, but HCOs have reason to be nervous. A study by the Ponemon Institute found that, following a data breach, 31% of customers severed their relationship with the vendor. Even if customers don't defect, most never trust the vendor the same way again. The Ponemon study found that 57% of customers had lost trust and confidence in vendors who notified them of breaches.⁹ Such a loss of reputation typically has long-lasting results, including decreased sales and increased marketing costs.

Looming Deadlines

Some HITECH measures, such as the direction of civil monetary penalties to the OCR, are effective immediately. Others will be phased in over time. The table on the next page summarizes some important HITECH deadlines.

8 http://www.frostbrowntodd.com/news_ca_hitech_act/

9 *Consumer's Report Card on Data Breach Notification*, Ponemon Institute, April 2008.

Date	HITECH Provision
Effective immediately	<p>The Office of Civil Rights can levy and receive fines.</p> <p>Civil monetary penalties are increased substantially.</p> <p>State Attorneys General are authorized to take action on behalf of aggrieved persons, even if their states have not established statutes authorizing such action; statutory penalties and attorney fees are recoverable.</p>
On or before September 15, 2009	Data breach notification rules take effect.
February 18, 2010	<p>A new Limited Data Set standard requires covered entities to release only the “minimum necessary” data.</p> <p>HIPAA coverage extends to business associates of HCOs.</p> <p>“Courier” firms require business associate agreements.</p> <p>Employees of HCOs and their business partners may have independent criminal liability for HIPAA violations.</p>
On or before February 18, 2011	<p>New prohibitions against disclosing PHI for remuneration go into effect.</p> <p>The Secretary of the HHS will impose mandatory civil monetary penalties for PHI violations involving “willful neglect.”</p>

The HITECH Act also defines other deadlines related to the security of Electronic Health Records (EHR). Because those deadlines are flexible, however, we haven’t listed them here.

Other Data Breach Notification Laws

As extensive as the new HIPAA privacy and security regulations are, they are not the only government regulations calling for organizations to secure PHI and to notify the public of PHI security breaches.

One of the most important data breach notification laws is a California law, the Security Breach Notification Act (SB 1386), which took effect in 2003. SB 1386 requires any business, regardless of its location, to publicly disclose the compromise of the private information involving a California resident. The original focus of SB 1386 was on private data such as a resident’s name, driver’s license number, and credit card number. In 2007, California legislature passed AB 1298, which extends the scope of SB 1386 to cover medical information and health insurance information as well.

While the new HITECH provisions in HIPAA require HCOs to disclose breaches affecting 10 or more individuals whom they have been unable to contact, the California data breach notification law requires disclosure of any breach affecting even a single California resident. Other states such as Illinois, whose data breach law took effect on January 1, 2006, similarly set the threshold for notification at the level of a single affected resident. The Massachusetts Data Privacy Law (also known as 201 CMR 17), scheduled to take effect in 2010, similarly enjoins HCOs and other business entities to protect private data and public disclose any breach affecting a single resident of the state.

As the Illinois and Massachusetts examples show, SB 1386 has become the model for data breach notification laws in other states and even other countries. As of the summer of 2009, forty-four U.S. states have enacted data breach notification laws. Twenty-five countries, including Canada and Japan, have also passed similar laws.

The FTC’s Data Breach Notification Law

The FTC has proposed a new security breach notification law for electronic health information. The law would apply to vendors such as WebMD and Google that sell online services based

on patient health records; the law specifically does not apply to entities already covered by HIPAA. Once finalized, this law would last until Congress passes legislation effecting similar regulations.

Another HHS Data Breach Notification Law

As of the summer of 2009, the HHS is developing a proposal for its own security breach notification law, similar to that proposed by the FTC, and independent of the breach notification rules included in HIPAA. Covered entities do not need to follow the HHS' guidance for protecting data, but if they do, they will gain safe harbor against the notification penalty.

Other Relevant Data Privacy Laws

In addition to data breach notification laws, data privacy laws compel organizations to protect the private data of citizens and consumers.

Federal laws include the Gramm-Leach-Bliley Act (GLBA) of 1999, which requires financial services firms to protect the private data of their customers. Another federal law, the Sarbanes-Oxley Act of 2002, requires that public companies protect and monitor access to material financial data. Its emphasis is on corporate data, rather than private data, but like data privacy laws aimed at consumers it has led data centers to deploy stricter access controls and authentication systems, which can be used to safeguard customer data as well.

In Canada, Europe, and Asia, governments have passed legislation requiring organizations to protect consumers' private information. Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) was passed in the late 1990's. In 2001, the legislation applied only to government regulated industries, such as airlines and broadcasting. In 2002, however, PIPEDA's coverage extended to the healthcare industry. Four Canadian provinces have also passed privacy laws that are similar to PIPEDA.¹⁰

Many U.S. states are following California's lead in mandating the protection of residents' private data. The Massachusetts Data Privacy Law, for example, takes effect on January 1, 2010, and requires that personal information about any Massachusetts resident be encrypted when stored or transmitted. It's a sweeping law, affecting businesses of all sizes and in all industries.

Nevada has passed a similar law (NRS 597.970) with regard to data transmission, requiring that any business in the state encrypt any private data it is transmitting electronically outside of the "secure system of the business."¹¹

But this law will expire on January 1, 2010, when a more sweeping data security law will take effect. Nevada's new security legislation requires all businesses storing or transmitting private data in the state to comply with the Payment Card Industry Data Security Standard (PCI DSS), a data security standard developed and adopted by the credit card industry. Nevada is the first state to require that all businesses, even sole proprietorships, accepting credit card payments in the state comply with PCI DSS. Some industry analysts consider this law a "game-changer."¹² Until now, government agencies have developed their own lists of security practices when mandating data protection. But PCI DSS is defined and controlled by an industry consortium, not a government agency. The Nevada legislature seems to recognize PCI DSS as a rigorous standard offering ready guidelines for security best practices, even if these guidelines are officially beyond government control.

It's possible that other states will copy Nevada's example and compel all businesses accepting credit card payments to comply with PCI DSS. (Minnesota already requires partial compliance in some situations.)

What's clear from all these laws, both national and regional, is that government agencies are taking an increasingly active role in establishing regulations to protect the private data of their residents. This trend is not likely to change any time soon.

10 http://en.wikipedia.org/wiki/Personal_Information_Protection_and_Electronic_Documents_Act

11 <http://www.leg.state.nv.us/NRS/NRS-597.html#NRS597Sec970>

12 http://www.bankinfosecurity.com/articles.php?art_id=1599&rf=070609eb

Where Does This Leave Enterprises in the Healthcare Industry?

The healthcare industry is witnessing some dramatic improvements brought about by technology, ranging from Wi-Fi tags for tracking the location of mobile patients to high speed networks for transmitting massive imagery files at lightning speed. As part of this transformation, healthcare organizations are making better use of email and the Internet. To reduce errors and to comply with new government regulations such as HIPAA, they're making more use of EMRs.¹³ The future of healthcare looks to be increasingly networked, electronic, and efficient.

Throughout this transformation, email will continue to be an essential application for communicating with patients, helping providers collaborate, and managing business processes such as billing. Whether for patient care or financial operations, email will continue to be used for transmitting PHI. In fact, as medical records move from paper to digital form, email will end up transmitting growing volumes of PHI.

Accordingly, enterprises must ensure that email carrying PHI is always secure and in compliance with the growing body of increasingly strict privacy regulations. Faced with new laws such as HIPAA and SB 1386 mandating encryption and the prompt disclosure of any significant security breach, enterprises cannot afford to tolerate any lapse at all in email security.

Requirements for Secure Email

Enterprises need a secure mail solution that is automated and comprehensive. IT departments can't afford to count on end users, in the daily rush of work, to distinguish sensitive data from insensitive data and take special steps to ensure that sensitive data is transmitted securely. It's far safer to build the automated detection of PHI into the email infrastructure itself. Upon detecting confidential information, such as diagnostic codes or credit card numbers, the email infrastructure itself should encrypt it automatically and deliver it to a valid recipient. Improper email should be blocked or quarantined for review by IT or security personnel.

The solution should be able to detect and protect confidential information, whether it's included in the body of an email message or in an attachment. Encryption, monitoring, and logging should accommodate treatment and business processes, providing a helpful service that interferes as little as possible with existing operations.

Smart Detection of PHI

This means detecting not only obvious identity information such as social security numbers and driver's license numbers. It also means detecting healthcare PHI such as diagnostic codes and admittance dates. To reduce false positive identification of PHI, it also means having technology smart enough to distinguish a 16-digit number that could be a credit card number from just any 16-digit number. (Credit card numbers follow certain formulas to facilitate account validation.)

Being able to distinguish a random sequence of numbers from a *meaningful* series of numbers—such as the digits in a social security number or a diagnostic code—requires so-called smart identification. A “smart identifier” is technology that distinguishes private data from non-private data (or, in HIPAA terminology, PHI from “de-identified information”) in a reliable, accurate way.

Smart identifiers reduce the number of “false positives” by the content scanning system. Encrypting non-PHI consumes computing resources and potentially creates operational overhead. By accurately distinguishing PHI from non-PHI, smart identifiers ensure that the email security infrastructure is as efficient as possible.

¹³ Research firm Kalorama Information estimates that the EMR market overall has reached \$9.5 billion. The market simply for EMR transfer equipment and applications—which would involve email and other electronic communications—will triple over the next five years, reaching \$1.6 billion by 2013. See “Market for EMRs pegged at \$1.6 billion by 2013”, Healthcare IT News, <http://www.healthcareitnews.com/news/market-emrs-pegged-16-billion-2013>

Standard and Custom Dictionaries for Private Data

While some data, such as credit card numbers and diagnostic codes, will require protection across the healthcare industry, other private data may assume forms that vary from company to company. A secure email solution should enable IT organizations to add algorithms (rules) for detecting proprietary account numbers or other custom IDs and to add their own internal dictionaries of data that require encryption or other special handling.

Rigorous Encryption

Any HIPAA-compliant email solution must apply rigorous encryption technologies to protect messages that carry sensitive data. Depending on where messages are flowing—within an organization’s secure network, between two servers on a secure partner network, or across the public Internet—it might be most practical to encrypt at the network perimeter, based on policies, rather than at the desktop, eliminating the need for end users to take any special steps when sending or receiving messages. In other situations, desktop-level encryption may be most appropriate. It’s important that an email solution not force an organization to dramatically change its workflow in order to accommodate security needs. The more flexible a solution is, the more likely it is to be adopted—and used—everywhere it’s needed.

To encrypt email messages, most email solutions rely on digital certificates. Alternatively, they might employ other approaches, such as identity-based encryption, deriving encryption keys from unique identities such as email addresses and obviating the need for distributing and managing digital certificates. In the choice of encryption technologies, too, offering an enterprise a range of choices is the best way to ensure that security measures are comprehensively implemented.

Flexible Deployment Scenarios

A growing number of enterprises are moving their inbound email filtering to a Software-as-a-Service solution running in the “cloud” (at one or more data centers managed by third parties). By processing inbound messages (90% or more of which are typically spam) on remote servers, these enterprises reduce the in-house computing resources (such as network bandwidth and storage) required by messages that will most likely be quarantined or discarded. They also minimize the security risk of email-borne malware wreaking havoc on internal systems. Finally, they avoid having to archive unwanted messages simply to comply with industry regulations compelling affected organizations to archive all email officially received by the organization.

Traditionally, filtering *outbound* messages for regulatory compliance and for data leak prevention has been performed in-house. This model ensures that no inappropriate content ever leaves the network perimeter.

But stringent data center security practices can make SaaS email filtering for outbound email just as viable as on-premises email filtering. Well-designed SaaS applications can be protected by rigorous security controls, including Transport Layer Service (TLS) encryption, the use of the Sender Policy Framework IDs as an anti-forgery safeguard, and stringent physical security controls certified by auditors to comply with best practices for SAS70 Type II.¹⁴ As a result, enterprises now have the option to filter both inbound and outbound email in the cloud, taking advantage of the scalability and low ownership costs associated with SaaS.

Another option for enterprises is a hybrid approach, using Software-as-a-Service (SaaS) processing for inbound email, while using on-premises processing for outbound email. A hybrid model is often a practical solution for enterprises interested in making a phased transition to all-SaaS filtering.

In addition to supporting these various deployment models, an email solution should offer a modular, plug-in architecture, so that enterprises can add functionality and tailor their own email solutions without shutting email operations down and deploying entirely new products.

14 SAS 70 is an auditing statement issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA). SAS 70 Type II evaluates whether controls were operating effectively during a period of review.

Archiving Capabilities to Comply with Record Retention Requirements

While this paper has focused primarily on the requirements for protecting private healthcare information during email transmission, HIPAA covered entities are also required to retain a wide range of documentation regarding their compliance with the regulation. In general, documentation must be retained for six years from the date of its creation, or the date of last effect, whichever is later (though some states mandate longer retention periods).

Documentation that must be retained includes:

- **Policy or procedural documentation:** Including notices of privacy practices, consents, authorizations and other standard forms
- **Patient requests:** Such as requests for access, amendment or accountings of PHI disclosures
- **Complaints:** Documentation related to the handling of patient and/or HCO employee complaints
- **Training:** Including processes for and content of workforce training.

An increasing number of email messages sent or received by HCOs could fall into these categories, and in some cases, may only exist in email (for example, patient requests sent via email). In a recent Proofpoint survey of large healthcare organizations, 68% of respondents cited “ensuring the confidentiality and protection of private healthcare information” as a top concern driving the need to archive email in their organizations.

HCOs should look for email security solutions that also include an email archiving component. Email archiving technology can ensure both the preservation and easy discovery of email messages that could be considered medical records or HIPAA-regulated documentation. Such systems should store email in an encrypted form, to ensure the security of any PHI contained in archived email messages and their attachments.

Security Rule Concerns and Email Archiving

With respect to archiving solutions themselves, the HIPAA security requirements around how such a system should be managed certainly apply. Given that it is inevitable that protected health information will make its way into an email archiving system, firms should ensure that their archiving implementation lives up to the security standards outlined in the HIPAA Security Rule.

For example, here are just a few of the procedural and technological approaches used in Proofpoint’s email archiving solution, Proofpoint ARCHIVE™, that customer usage of the solution complies with their obligations under the HIPAA Security Rule:

- **Administrative safeguards:** Proofpoint ARCHIVE is SAS 70 Type II certified. SAS 70 is an industry standard process in which a service provider formally documents its procedures. This documentation is reviewed by a third party auditor to verify that the documentation is current and complete, as well as confirming that the service provider is following the stated procedures.
- **Physical safeguards:** The Proofpoint ARCHIVE service is operated in world-class collocation facilities with biometric access controls and redundant environmental protection systems. In addition, Proofpoint ARCHIVE’s patented DoubleBlind Encryption™ technology encrypts data using a unique key that only the customer holds.
- **Technical safeguards:** Proofpoint ARCHIVE’s DoubleBlind Encryption ensures that only the customer, as the sole holder of the decryption key, can access archived data. The solution integrates directly into Active Directory in the customer environment to leverage the existing access procedures and controls put in place by the customer. Access to the system is fully audited. Additionally, Proofpoint ARCHIVE generates digital fingerprints (MD5 signatures) at various points in the archival process and recalculates these signatures on a regular basis to ensure the ongoing integrity of archived data. A copy of the data is stored at a geographically separate location for recovery purposes.

Requirements Summary

The table below summarizes some of the requirements for a regulatory-compliant secure email system for healthcare.

Requirement	Benefit
Comprehensive detection of private data: <ul style="list-style-type: none">○ Pre-defined and custom dictionaries○ Smart identifiers (reduces false positives)○ Support for scanning and encrypting attachments	Ensures that all private and sensitive data is identified for secure treatment
Rigorous encryption	Protects PHI and other sensitive data from interception and corruption.
Policy-based controls	Enables IT organizations to adapt the secure email solution to their organization's requirements and workflows.
Flexible remediation: ability to encrypt, redirect, quarantine, block, add X-header, or annotate messages, as needed	Enables IT organizations to adapt the secure email solution to their organization's requirements and workflows.
Reporting to discover potential issues and to demonstrate compliance	Meets HIPAA requirements for reporting and monitoring. Aids employee training on security.
Flexible deployment models to meet different customer needs: <ul style="list-style-type: none">○ SaaS○ On-premises appliances○ Hybrid deployment options○ Modular architecture	Adapts security implementations to the varied needs of organizations and even to the varied needs among branch offices within an organization.
Archiving capabilities	Ensures that email that constitutes medical records or HIPAA-regulated documentation is retained for the proper period and can be easily retrieved if required.

Conclusion

Judging from both the HITECH Act included in the stimulus bill and the FTC's multi-million dollar penalty against CVS, this much is clear: the U.S. federal government has gotten serious about enforcing HIPAA security regulations. At the same time, state governments are demonstrating their own fervor for data security by enacting privacy laws modeled on California SB 1386. These new laws, such as the Massachusetts Data Privacy Law taking effect on January 1, 2010, compel enterprises to protect individuals' data at rest and in motion and to disclose any security lapse, even small lapses that previously would have been overlooked.

By taking steps now to implement automated, comprehensive email security, healthcare organizations and their business partners can reap the undisputed operational benefits of email communications, while avoiding the public censure and financial penalties that might result from regulatory action.

A flexible email security solution should readily accommodate the IT architecture, business operations, and regulatory requirements of any healthcare enterprise today, while preparing that enterprise to benefit from electronic medical records and other exciting IT advances in the near future.

For Further Reading

Proofpoint offers a variety of free educational whitepapers that further describe the legal, financial and regulatory risks associated with outbound email and the policies, processes and technologies that can be used to reduce those risks. Visit our online resource center at <http://www.proofpoint.com/resources> for the latest information.

The Critical Need for Encrypted Email and Secure File Transfer Solutions

This whitepaper from Proofpoint and Osterman Research discusses key issues around the encryption of both email and file transfer systems, some of the leading statutes that require sensitive content to be encrypted, and suggestions for moving forward with encryption:

<http://www.proofpoint.com/id/osterman-encryption-wp/index.php>

Outbound Email and Data Loss Prevention in Today's Enterprise

A summary of Proofpoint's annual research on outbound email and content security issues. Reports statistics on many on the prevalence of data breaches via email, the web and other channels; enterprise concerns about protecting confidential information; and the techniques and technologies enterprises have used to mitigate outbound email risks:

<http://www.proofpoint.com/outbound>

Global Best Practices in Email Security, Privacy and Compliance

This whitepaper discusses the impact of the latest global regulations that impact the email security policies and strategies of today's enterprises, universities and government organizations.

<http://www.proofpoint.com/id/email-security-best-practices-wp/index.php>

Email Archiving: A Proactive Approach to eDiscovery

This whitepaper addresses the key e-discovery challenges facing legal and IT departments today, including the impact of regulations such as the Federal Rules of Civil Procedure (FRCP) and how email archiving technology can help your organization be better prepared:

<http://www.proofpoint.com/id/email-archiving/index.php>

Leveraging SaaS Technology to Reduce Costs

These whitepapers from Proofpoint and Osterman Research discuss how Software-as-a-Service solutions for email security and email archiving can greatly reduce costs—without sacrificing the security of your organization's most valuable data:

Using SaaS to Reduce the Costs of Email Security

<http://www.proofpoint.com/id/saas-email-security-costs-whitepaper/index.php>

Email Archiving: Realizing the Cost Savings and Other Benefits from SaaS

<http://www.proofpoint.com/id/saas-email-archiving-costs-whitepaper/index.php>

About Proofpoint, Inc.

Proofpoint secures and improves enterprise email infrastructure with solutions for email security, archiving, encryption and data loss prevention. Proofpoint solutions defend against spam and viruses, prevent leaks of confidential and private information, encrypt sensitive emails and archive messages for retention, e-discovery and easier mailbox management. Proofpoint solutions can be deployed on-demand (SaaS), on-premises (appliance), or in a hybrid architecture for maximum flexibility and scalability.

Proofpoint Solutions for Outbound Email Content Security, Data Loss Prevention and Regulatory Compliance

Proofpoint's SaaS, appliance, virtual appliance and software solutions for email security and data loss prevention defend against all types of inbound and outbound message-borne threats.

Enforcing Email Acceptable Use Policies

Proofpoint makes it easy to define and enforce corporate acceptable use policies for message content and attachments. A convenient point-and-click interface simplifies the process of defining complex logical rules related to file types, message size, and message content. Proofpoint's content compliance features can be used to identify and prevent a wide variety of inbound and outbound policy violations—including offensive language, harassment, file sharing, and violations of external regulations. Non-compliant messages can be acted on with a wide variety of options, including quarantine, reroute, reject, annotate, and other actions.

Preventing Leaks of Confidential and Proprietary Information

As email has become the most important communication channel in today's enterprise, email systems have become the main repository for sensitive, confidential, and mission-critical information. The Proofpoint Digital Asset Security™ module keeps valuable corporate assets and confidential information from leaking outside your organization via email. Powerful Proofpoint MLX™ machine learning technology analyzes and classifies your confidential documents and then continuously monitors for that information in the outbound message stream—stopping content security breaches before they happen.

Ensuring Compliance with Data Protection and Privacy Regulations

The Proofpoint Regulatory Compliance™ module protects your organization from liabilities associated with data protection and privacy regulations such as HIPAA, GLBA and PCI. Pre-defined rules automatically scan for non-public information, including protected health information and personal financial information, and act on non-compliant communications, rejecting or encrypting messages as appropriate.

Enabling Policy-based Encryption

Proofpoint's SaaS, appliance and software solutions for email security can all optionally be equipped with robust, policy-based encryption features that automatically encrypt individual messages based on an organization's policies, without requiring end-users to take any special actions. Proofpoint's flexible rules, managed dictionaries and "smart identifiers" are used to accurately detect non-public information—such as protected health information and personal financial information—and reject or encrypt messages as appropriate.

<http://www.proofpoint.com/encryption>

Protecting HTTP and FTP Streams: Multi-protocol Content Security

The Proofpoint Network Content Sentry™ extends Proofpoint's email protection to additional messaging streams, including HTTP and FTP. This module inspects all outbound network traffic in real-time, monitoring for confidential information, private customer or employee data (including private healthcare, financial or identity information) and other sensitive content that may leak outside the enterprise.

Archiving Email for eDiscovery Readiness, Compliance and Easier Mailbox Management

Proofpoint ARCHIVE™, a SaaS email and IM archiving solution, incorporates Proofpoint's patented DoubleBlind Encryption™ technology, which encrypts messages before transmission to Proofpoint's datacenters where they are stored in encrypted form. At the same time, Double-Blind Encryption ensures that data remains fully searchable via the secure Proofpoint ARCHIVE appliance. Proofpoint ARCHIVE helps organizations be prepared for eDiscovery events, improves end-user access to historical email and ensures compliance with your organization's email retention policies.

<http://www.proofpoint.com/emailarchiving>

Eliminating Risks Associated with FTP and Email Transmission of Large or Confidential Files: Secure File Transfer

Proofpoint Secure File Transfer™ lets end users send large files (or files that require enhanced security) easily and securely—while minimizing the impact of large attachments on your email infrastructure.

<http://www.proofpoint.com/sft>

©2009 Proofpoint, Inc. All rights reserved.
Proofpoint, Proofpoint ARCHIVE, Proofpoint ENTERPRISE, Proofpoint Secure File Transfer, Proofpoint Protection Server, Proofpoint Messaging Security Gateway, Proofpoint on Demand, Proofpoint MLX, Proofpoint Content Compliance, Proofpoint Regulatory Compliance, Proofpoint Network Content Sentry, Proofpoint Secure Messaging, DoubleBlind Encryption and Proofpoint Digital Asset Security are trademarks or registered trademarks of Proofpoint, Inc. in the US and other countries.
Version 08/09 - Rev A

For More Information

Proofpoint, Inc. US

Worldwide Headquarters

892 Ross Drive
Sunnyvale, CA 94089
USA
P 408 517 4710
F 408 517 4711
E info@proofpoint.com
www.proofpoint.com

Proofpoint, Inc. EMEA

Proofpoint, Ltd.
The Oxford Science Park
Magdalen Centre
Robert Robinson Avenue
Oxford, UK
OX4 4GA
Tel +44 (0) 870 803 0704
Fax +44 (0) 870 803 0705
E info@proofpoint.com
www.proofpoint.com

Proofpoint, Inc. Asia Pacific

5th Floor, Q.House Convent Bldg.
38 Convent Road, Silom, Bangrak
Bangkok 10500, Thailand
Tel +66 2 632 2997
E info@proofpoint.com
www.proofpoint.com

Proofpoint Japan K.K.

906 BUREX Kojimachi
Kojimachi 3-5-2, Chiyoda-ku
Tokyo, 102-0083
Japan
P +81 3 5210 3611
F +81 3 5210 3615
E sales-japan@proofpoint.com
www.proofpoint.co.jp

Proofpoint, Inc. Canada

60 Adelaide Street East, 9th Floor
Toronto, Ontario M5C 3E4
Tel +1 416 366 6666
Fax +1 416 366 6667
E info@proofpoint.com
www.proofpoint.com

Proofpoint, Inc. Mexico

Uxmal 165 int 7
Col. Narvarte
CP 03020
México D.F.
Tel: +52 55 5330 3382
E info@proofpoint.com
www.proofpoint.com