

Stop PHI Leaks:

A Guide to the Importance of Email Encryption and HIPAA

INSIDE:

- > PHI exposure
- > Recognizing PHI in email
- > Tougher HIPAA enforcement
- > Content filter development and accuracy

A Whitepaper Published November 2009 by



Table of Contents

| | |
|---|----|
| Overview | 3 |
| PHI leaks more common than you think..... | 4 |
| PHI in email defined | 4 |
| Tougher HIPAA enforcement and higher penalties..... | 8 |
| Policies not good enough | 8 |
| Content filters using strong lexicons | 8 |
| Content filter development and accuracy | 9 |
| How content filtering is implemented | 9 |
| Conclusion..... | 10 |
| About ZixCorp | 11 |

Overview

If you're not protecting your patients' personal health information (PHI), be prepared to pay the price.

The revamped Health Insurance Portability and Accountability Act (HIPAA) comes down hard on healthcare organizations and their business partners if they don't rigorously protect PHI.

The Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of American Recovery and Reinvestment Act of 2009 (ARRA), calls for the encryption of all PHI sent via email.

The most popular way to exchange information is email. It's well understood and it's ubiquitous. However, its inherently insecure nature, combined with it being a high volume channel, makes it particularly susceptible to HIPAA-related exposures, especially as it's frequently used to send sensitive data containing PHI.

The healthcare industry and its business partners face significant challenges to meet the compliance requirements of the revised HIPAA. This legislation imposes new security rules that provide substantial authority for enhanced enforcement. Breaking the rules will cost you. Under the new legislation, organizations will be fined up to \$1.5 million—up from \$25,000—for violating patients' privacy. It also extends the effective reach of HIPAA coverage to business associates. Companies must re-evaluate their overall privacy compliance programs and implement more effective information security practices, including encryption wherever possible.

ZixCorp recognizes that many healthcare organizations are just beginning to implement effective methods to ensure private information is transmitted securely. Each day healthcare organizations unknowingly expose themselves to significant risks posed by emailing unprotected data—even with privacy policies in place.

ZixCorp uses the industry's leading comprehensive healthcare content filters to help identify an organization's PHI exposure while ensuring their emails are secured. This guide illustrates what emailed PHI looks like and explains how ZixCorp's content filters, based on strong HIPAA-related lexicons, are part of an effective and thorough secure email protection program.

PHI Leaks Are More Common Than You Think

ZixCorp is the dominant provider of policy-based email encryption to the healthcare industry. Healthcare enterprises and their business associates are an important part of our business. One out of every seven hospitals in the United States uses ZixCorp for email encryption. ZixCorp's health insurance providers protect the lives of more than 85 million people.

To help businesses monitor their security performance, ZixCorp offers the ZixAuditor®. This service assesses an organization's email traffic, searches for PHI and highlights privacy risks.

ZixCorp has sampled more than eight million emails sent from or received by 73 healthcare organizations including insurance plans, hospitals, physician practices and intermediaries. None had email encryption in place—every single one had unsecured PHI in their email.

For each of the organizations studied, the average exposure rate in outbound emails was between two and five per cent. Though the number may seem low, here's the reality—a small-to medium-sized healthcare organization might send 5,000 emails per week. If the average exposure rate is, conservatively, two per cent, that's 100 occurrences of unsecured PHI escaping each week, or 5,000 occurrences per year. Large organizations typically send more than 10,000 messages per day. At the two per cent rate, that's approximately 50,000 occurrences of unsecured PHI leaving per year. With punitive fines of up to \$1.5 million, that could spell financial disaster.

10,000 messages per day
x 2% exposure rate
= 50,000 occurrences of
unsecured PHI per year.

PHI in email defined

What does PHI look like? An examination of messages identified as containing PHI reveals that most are not malicious efforts to expose confidential information. The bulk is between organizations using email in the daily course of business.

Most of the messages are administrative or clerical in nature—clarifying patient records and fixing billing issues. They're conversations between providers and payors discussing individual claims, correcting coding issues, or querying dates.

Some of the messages deal with patient treatment—providers communicating with each other about a referral, consulting on a diagnosis, or a shared patient.

Additionally, patients communicate with care providers via email (and vice versa) asking questions, clarifying medications, and scheduling appointments.

Here are some examples of email messages containing PHI:

EXAMPLE #1

From: Sue@sender.net
To: Linda@recipient.net
Subject: Shared patient

Here's the info you requested on patient Jane Doe, ss# 999-99-9999. She began tamoxifen approximately 5/15/2009. No sign of cancer.

Example #1 is clear, concise and easily fits HIPAA's definition of PHI. It contains a patient's Social Security Number, medication, and diagnosis discussion.

EXAMPLE #2

From: John@sender.net
To: Bob@recipient.net
Subject: Where is this?

Hello, could you check on this claim, mem no12345 for 39.55, dates of svc from 013008 through 051609.
Sent appeal on 0809 with prime pymt, did you receive, is this in process?

This is a common example of an email containing PHI. It is cryptic, full of abbreviations, sentence fragments and misspellings. Some may argue this is not an example of PHI because it doesn't list the patient's name. HIPAA's definition of PHI includes any information that identifies an individual and if there is a reasonable basis to believe the data points to them.

Certainly, in many information systems, a member or patient identification number can more accurately pinpoint a person's identity than their name alone. There may be multiple patients with the same name, but they each have a unique ID in the health information system.

EXAMPLE #3 – Sample Email Attachment

Patient Name: Jane Doe

Admitted: 11/1/09

Therapist: J. Smith LMFT

DSM-IV

AXIS I 311 Depressive Disorder NOS

304.80 Polysubstance Dependence

313.81 Oppositional Defiant Disorder

300.00 Anxiety Disorder NOS

TREATMENT ISSUES:

Jane Doe was admitted to the program with complaints by parents of several symptoms. Reports included self-harming behavior (in the form of substance abuse and cutting).

[This specific report continued for several pages in detail...]

Example #3 shows an excerpt from an email attachment. In this case, it is a document that contains a patient's medical history shared by two therapists. It includes the DSM-IV classifications relevant to the case and a very detailed history extended over several pages.

Because it relates to a patient's mental health, it is especially sensitive.

EXAMPLE #4 – Sample Email Attachment

| <u>GRP#</u> | <u>SSN</u> | <u>LAST NAME</u> | <u>FIRST</u> | <u>SRV DATE</u> | <u>ACCT BAL</u> |
|-------------|-------------|------------------|--------------|-----------------|-----------------|
| 111111 | 999-99-9999 | AALTO | T | 00/00/00 | \$167.72 |
| 111112 | 999-99-9999 | ABARE | B | 00/00/00 | \$672.00 |
| 111113 | 999-99-9999 | ABARE | D | 00/00/00 | \$4,633.00 |
| 111114 | 999-99-9999 | ABARE | W | 00/00/00 | \$1,165.00 |
| 111115 | 999-99-9999 | ABDELHAMED | A | 00/00/00 | \$272.07 |
| 111116 | 999-99-9999 | ABDELHAMED | A | 00/00/00 | \$272.07 |
| 111117 | 999-99-9999 | ABDELHAMED | E | 00/00/00 | \$7,932.65 |
| 111118 | 999-99-9999 | ABDELHAMED | E | 00/00/00 | \$7,932.65 |
| 111119 | 999-99-9999 | ABDELHAMED | Z | 00/00/00 | \$28.02 |
| 111120 | 999-99-9999 | ABDELHAMED | Z | 00/00/00 | \$28.02 |
| 111121 | 999-99-9999 | ABRAHAMSON | P | 00/00/00 | \$15,626.94 |
| 111122 | 999-99-9999 | ABRAHAMSON | P | 00/00/00 | \$32.74 |
| 111123 | 999-99-9999 | ABRAHAMSON | R | 00/00/00 | \$485.49 |
| 111124 | 999-99-9999 | ABRAHAMSON | R | 00/00/00 | \$25,637.43 |
| 111125 | 999-99-9999 | ABRAMS | A | 00/00/00 | \$14,268.06 |
| 111126 | 999-99-9999 | ABRAMS | C | 00/00/00 | \$350.00 |
| 111127 | 999-99-9999 | ABRAMS | J | 00/00/00 | \$630.53 |
| 111128 | 999-99-9999 | ABRAMS | L | 00/00/00 | \$2,548.20 |
| 111129 | 999-99-9999 | ABRAMS | M | 00/00/00 | \$23,272.10 |
| 111130 | 999-99-9999 | ABRAMS | S | 00/00/00 | \$5,136.71 |
| 111131 | 999-99-9999 | ABUAN | E | 00/00/00 | \$41,206.27 |
| 111132 | 999-99-9999 | ABUAN | M | 00/00/00 | \$2,231.36 |
| 111133 | 999-99-9999 | ABUAN | S | 00/00/00 | \$1,220.61 |

[This specific attachment continued for hundreds of rows...]

Example #4 is the kind of message that makes privacy officers cringe. This is another excerpt from an attachment. In this case, it's a spreadsheet that lists patients' Social Security numbers, names, dates of service, and account balances.

Messages with attachments like this are data files of patient accounts usually shared between providers and business associates responsible for collections or claim processing. They are particularly sensitive because a single message could contain the private information of thousands of individuals.

This is a good example of how a single instance of exposure can cause enormous liability for the organization and pose great risk to patient privacy.

Protecting this type of information is extremely important under the new HIPAA legislation, especially when it involves communication with business partners not previously required by HIPAA to secure personal data.

Tougher HIPAA enforcement and higher penalties

In brief, the goal of the HIPAA Security Rule is to protect the confidentiality, integrity and availability of electronic PHI. If your organization is caught emailing unencrypted PHI, you may:

- Face fines of up to \$1.5 million
- Be required to contact those whose privacy has been affected.
- Be required to notify the media that you have caused a security breach.

State Attorneys General now have clear and explicit authority to enforce HIPAA's rules. More than \$24 million of federal dollars made available through American Recovery and Reinvestment Act (ARRA) will be spent on enhanced enforcement.

For more information, visit: <http://www.hhs.gov/ocr/privacy/>

Policies alone are not enough

Most healthcare organizations send unsecured PHI in their email, even when they have administrative policies in place to deter this. These fall short of protecting PHI. The most effective way to secure PHI includes policies and a trusted safeguard such as policy-based email encryption using a proven healthcare filter.

With enhanced enforcement of tough new HIPAA requirements, compliance is crucial. However, ZixCorp studies show that some organizations continue to include unsecured PHI in their emails. Why would they take this risk?

- They may not recognize there is a legal requirement to provide protection for PHI in email. It's easy to overlook email because it's not an "official" business process, although it's used as a convenient and fast way to share data.
- They may have administrative policies and some encryption technology in place, but the two aren't working cohesively to provide an effective solution.

Content filter solutions using strong lexicons

A lexicon is a file consisting of a comprehensive set of terms, phrases, expressions and numeric patterns that identify sensitive information. ZixCorp has developed lexicons specifically for healthcare organizations to automatically detect and encrypt messages containing PHI.

ZixCorp uses many sources to generate the healthcare lexicon that searches for PHI, including federal regulations, authoritative reference sources and "standard of care" practices. ZixCorp's content scanners examine all message subjects, bodies and attachments for expressions defined within the lexicon.

Content filter development and accuracy

ZixCorp goes to great lengths to develop lexicons that are accurate and precise. This is accomplished through comprehensive definition and design, coupled with exhaustive manual analysis, to ensure the lexicons' results agree with the judgment of the designers. The following is an overview of the design process and validation of the healthcare lexicons:

Lexicons are designed based on the PHI definition from HIPAA regulations.

- Hundreds of thousands of message samples are gathered from payors and providers.
- The message samples are manually examined and classified.
- Reference sources are identified and used to ensure comprehensive content.
- The lexicons are constructed from the terminology lists and run against sample messages.
- The lexicons' results are compared to the results of the manual classifications.
- Lexicons are tuned against the samples, and measured against separate samples to ensure real-world accuracy performance.
- Ongoing revisions are made based on ZixAuditor analyses and customer input.

With each new release, the accuracy of the healthcare lexicons has improved, minimizing the occurrence of false hits. The end result is a precise, accurate and comprehensive content scanner.

How content filtering is implemented

The healthcare lexicons are an integral part of ZixAuditor® email assessment and ZixCorp's email encryption service. The lexicons ensure that PHI is detected and encrypted for all email throughout an organization.

ZixAuditor is a comprehensive service that helps organizations identify email vulnerabilities, implement more effective policies and procedures, and monitor ongoing communications to determine compliance and effectiveness. The healthcare lexicons detect PHI in both incoming and outgoing messages.

ZixVPM is a server-based enterprise encryption solution that provides a secure e-messaging gateway without the need to create, deploy or manage end-user encryption keys and software. The healthcare lexicons eliminate human guesswork and enforce existing company security policies for total email protection.

Conclusion

Email is a high volume communications channel. Even a small percentage of unsecured PHI quickly mounts to a large risk. Sending or receiving unencrypted email containing sensitive data compromises patient privacy. Under HIPAA's new rules, an organization will be held accountable, with repercussions to its reputation and its bottom line. The greater the volume of email, the higher the risk.

ZixCorp offers everything an organization needs to detect PHI in email and secure it in accordance with HIPAA. Only ZixCorp offers a comprehensive suite of services to ensure email compliance—an email assessment service, built-in healthcare lexicons to detect PHI, and a user awareness program to ensure that employees and email recipients understand company email policy. For more information about ZixCorp's services, call toll-free 866-257-4949 or visit www.zixcorp.com.

About ZixCorp

ZixCorp® provides easy-to-use-and-deploy e-communications services that protect, manage and deliver sensitive PHI. Its email encryption service includes:

ZixVPM® (Virtual Private Messenger) is a system-wide solution for organizations that require a high level of protection for email communications. It seamlessly integrates into existing network infrastructure, solves the need for security and enables companies to set their e-messaging policies for the entire enterprise, departments or individuals.

ZixAuditor® is a non-intrusive email analysis service that helps organizations identify email security vulnerabilities, monitor ongoing communications to determine compliance and implement more effective policies if needed. ZixAuditor provides strategic insight into email use to help companies better understand email usage patterns.

ZixPort® is a Web-based secure e-messaging portal that provides enterprises with private, secure and branded communication capabilities while minimizing the impact to existing IT, Web or security infrastructures.

ZixMail® is a desktop encryption program that provides point-to-point secure email delivery. It's an easy-to-use manual solution that lets users encrypt, decrypt and send private emails and attachments to anyone.

ZixDirect® is a delivery method that makes it possible to push an encrypted e-mail directly to a user's inbox. With ZixDirect, there is no client software to install or maintain, and the user does not need to have any encryption capabilities to read the message. Users receive secure emails directly in their inbox and have the ability to read secure messages while working offline.

ZixDirectory® is the largest email encryption directory in the world. It enables seamless and secure communication among its millions of members by providing a centralized directory for automated key exchange. As an added service provided with ZixVPM and ZixMail, ZixDirectory enables users to transparently send and receive encrypted emails without having to exchange certificates. In addition, when used with either ZixVPM or ZixMail, ZixDirectory makes it possible to send secure emails to anyone, anywhere, without pre-registration or configuration.

ZixConnect® is a managed TLS service that allows companies to secure their email communication to multiple partners using a single TLS connection. ZixConnect is for organizations that need to secure email communications with key business partners, but are concerned about the long-term complexity of managing multiple separate TLS connections.