WHITE PAPER

Stop PHI Leaks Now: A HIPAA Survival Guide

ZIXCORP | FEBRUARY 2005

zixresearch center

INSIDE:

- PHI exposure
- Recognizing PHI in email
- The HIPAA Security Rule
- Content scanning solutions via lexicons
- Lexicon development and accuracy

zixcorp

Table of Contents

Overview

Email is an important business tool and a slippery slope when it comes to compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA requires "reasonable and appropriate safeguards" whenever emailing Protected Health Information (PHI), but ongoing studies conducted by Zix Corporation show that healthcare organizations are still in the early stages of adopting effective methods to ensure private information is transmitted securely.

The ZixCorp® studies demonstrate that many healthcare organizations unknowingly expose themselves to the significant risks posed by unprotected email — even with email privacy policies in place. But how can the healthcare community accurately keep confidential information private?

ZixCorp's e-messaging protection services utilize comprehensive and accurate healthcare lexicons to help identify an organization's PHI exposure and to ensure those emails are secured. This white paper illustrates what emailed PHI looks like and explains how ZixCorp's proven lexicons are part of an effective secure email protection program.

PHI Leaks Common

As a provider of secure e-communication services, ZixCorp is profoundly interested in the nature and dynamics of email within the healthcare community, between business associates, and their customers or patients.

To help understand the nature of these communications, ZixCorp has developed the ZixAuditor® assessment service that provides a characterization of an organization's email traffic and PHI content.

Using this service over the past two years, the email streams of hundreds of healthcare organizations have been analyzed to assess the level of PHI exposure and the risk to patient privacy.

ZixCorp sustains an ongoing study of email sampled from healthcare organizations. These samples represent the inbound and outbound email traffic for a period of three to seven days for each of the organizations that commission assessments. The messages are filtered through ZixCorp's healthcare lexicon which identifies PHI, manually sampled for accuracy, and classified as containing sensitive PHI or not. Only those messages containing PHI are considered a risk to the organization and patient privacy.

Between April and December 2004, ZixCorp sampled over eight million emails sent from or received by 73 healthcare organizations including health insurance plans, hospitals, physician practices, intermediaries, and other healthcare-related organizations. None of the organizations examined had secure e-messaging solutions in place.

All the organizations examined during this time period had unsecured PHI in their email. It's not surprising that organizations have this kind of exposure given the universality of email and the convenience it supplies in day-to-day operations. But the messages pose potential liability risks and are not in compliance with HIPAA's Security Rule.

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

For each of the organizations studied, the average exposure rate in outbound email flow was approximately 2%. Though the number may seem low, here's the reality: a small- to medium-sized healthcare organization might send 5,000 messages out of the organization per week. At the average 2% exposure rate, that's 100 occurrences of unsecured PHI leaving the organization each week. That's 5,000 occurrences per year. Large organizations can send over 10,000 messages per day. At the 2% average exposure rate, that's approximately *50,000 occurrences of unsecured PHI leaving the organization per year.*

What PHI in Email Looks Like

What does this PHI look like? Manual examination of messages identified as containing PHI reveals that most are not malicious efforts to expose confidential information. The bulk of these messages are between organizations using the email channel 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, clarifying dates, etc.

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

Additionally, some messages are direct communications between patients and care providers. Patients communicate with care providers via email (and vice versa) asking questions, clarifying medications, managing their disease, scheduling appointments, and other things of this nature.

Below 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 5/15/2002.
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 chk on this claim, mem num 12345 for 1283.15,
dates of svc from 0130004 through 051604.

Sent appeal on 0806 with prime pymt, did you receive, is this
in process?
```

Example #2 is more common to what is seen in email containing PHI. It is cryptic, full of strange abbreviations, sentence fragments and misspellings. Building tools that scan for PHI in email can be challenging because of these kinds of messages. It speaks to the nature of email as a communication method. It's free, open text.

Some readers may argue that this example is not PHI because it does not list the patient's name. But HIPAA's definition of PHI is general and includes any information that identifies the individual or if there is reasonable basis to believe the information can be used to identify the individual.

Certainly, in many information systems, a member number, patient ID or other such account number is more individually identifying than a person's name. 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 : 1/1/05
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 being shared between two therapists. It includes the DSM-IV classifications relevant to the case and a very detailed history that extended over several pages.

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

EXAMPLE #4 – Sample Email Attachment

GRP#	SSN	LAST NAME	FIRST	SRV DATE	ACCT BALANCE
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 shows what is all too common in the email examined by ZixCorp. It's 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 patient Social Security numbers, names, dates of service, and account balances.

Messages with attachments like this are data files of patient accounts usually being 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 potentially 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.

All these examples are from email conversations taking place between covered entities, meaning that the disclosures are permitted under the HIPAA Privacy Rule. However, because these messages were sent via email across the Internet (an inherently insecure method of transmission), the messages do not meet the HIPAA Security Rule requirements specifying the need to encrypt PHI when sending across a public network.

✔ WHAT IS THE SECURITY RULE?

In brief, the goal of the HIPAA Security Rule is to protect the confidentiality, integrity and availability of electronic PHI. Each security requirement in the rule can be categorized into one of three groups:

- Administrative safeguards
- Physical safeguards
- Technical safeguards

It is in the last category where securing email resides.
To view the full Security Rule,
visit http://www.aspe.hhs.gov/admnsimp/FINAL/FR03-8334.pdf

Policies Alone Are Not Enough

This is the heart of the issue: most healthcare organizations send unsecured PHI in their email, even when they have administrative policies in place requiring users to not send PHI via email. Administrative email policies alone simply fall short of protecting PHI. The ZixCorp studies demonstrate this. A combined approach that includes both policies and technical safeguards is simply more effective.

With the deadline for HIPAA Security Rule compliance looming in April, obviously a disconnect exists between what HIPAA requires and the fact that most organizations are sending unsecured PHI in their email. What are some of the implications of this continued behavior?

1. Organizations may not recognize that there is a legal requirement to provide protections for PHI in email. It's easy to overlook email because it's not an "official" business process, although clearly it's being used as such.

2. Some organizations have administrative policies in place and adequate technology, but they are not working together to form an effective solution.

3. Some organizations have underestimated the importance of user awareness and training. Even the best policies and technology will fail if no one knows how or when to use them.

Administrative policies can fail because they alone are not sufficient to protect PHI in today's ubiquitous email environment. But technical solutions are not sufficient either. Technical systems that end users misunderstand, misuse, or ignore also will fail.

Systems and policies cannot work in isolation. They must be combined and used in conjunction with appropriate procedures, user training, and ongoing risk assessment. A successful union of email encryption technology, user training, and administrative policies enables organizations to most effectively meet the regulatory compliance, safeguard themselves, and avoid the risk of exposing PHI. Doing so can secure the email channel, ensuring that it remains a viable asset to the organization and not a liability sinkhole.

Content Scanning Solutions via Lexicons

A lexicon is a file consisting of a comprehensive set of terms, phrases, expressions, and numeric pattern masks that identify sensitive types of information. ZixCorp has developed lexicons specifically for healthcare organizations to automatically detect and encrypt messages like those shown above.

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

Lexicon Development and Accuracy

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

1. ZixCorp consulted with expert legal counsel in regulatory compliance at Preston-Gates-Ellis, LLP.
2. Lexicons were designed based on the definition of PHI from HIPAA regulations.

3. Tens of thousands of message samples are gathered from payors and providers.
4. The message samples are manually examined and classified.
5. Reference sources were identified and used to ensure comprehensive content. These sources included:
   - National Library of Medicine's Medical Subject Headings (MeSH) for human diseases and diagnoses
   - American Medical Association's Current Procedural Terminology (CPT)
   - Center for Disease Control's International Classification of Diseases v.9 (ICD-9)
   - Medicare's Health Care Procedural Coding System (HCPCS)
   - American Insurance Association of America glossary
6. The lexicons were constructed from the terminology lists and run against sample messages.
7. The lexicons' results are compared to the results of the manual classifications.
8. Lexicons are tuned against the samples, then measured against separate samples to ensure excellent real-world accuracy performance.
9. 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 and maximizing the liability coverage. The end result is a precise, accurate, and comprehensive content scanner that can correctly identify PHI in email.

How the Lexicon is Implemented

The healthcare lexicons are an integral part of ZixAuditor® email assessment and ZixVPM® (Virtual Private Messenger) email encryption services. The lexicons ensure that PHI is detected and encrypted for all email throughout an organization.

ZixAuditor is a comprehensive service that enables organizations to identify email vulnerabilities, implement more effective policies and procedures, and monitor ongoing communications to determine compliance and effectiveness. The healthcare lexicon detects PHI in both incoming and outgoing messages for a total picture of the effectiveness of current procedures.

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 channel, so even a small percentage of unsecured PHI can quickly mount to a large risk. While it may be possible to send an occasional unsecured email in response to specific circumstances without much risk, any routine or reasonable high-volume use of email will create serious risks to organizational liability and patient privacy. The greater the volume of email, the higher the risk, and the more evidence is available against the organization in case of a penalty action.

ZixCorp's e-messaging protection services offer everything a company needs to detect PHI in email and secure it in accordance with the HIPAA Privacy and Security Rules. 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 on ZixCorp services, call toll-free **866-257-4949** or visit **www.zixcorp.com**.

About ZixCorp

ZixCorp® provides easy-to-use-and-deploy e-communication services that protect, manage, and deliver sensitive HIPAA information. Hundreds of healthcare organizations use ZixVPM®, a corporate-wide email encryption service that automatically encrypts email messages containing PHI. Other services include content filtering, e-prescribing and e-lab services for improved office efficiency. ZixCorp e-messaging protection services include:

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 enables organizations to 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 enables users to encrypt, decrypt, and send private emails and attachments to anyone.

2711 N. Haskell Ave.
Suite 2300, LB 36
Dallas, TX 75204
1-866-257-4949
www.zixcorp.com

PHIWP205