



## Assessing PHI Risks in Email

Today, e-mail has become both an important business tool and a slippery slope when it comes to compliance with HIPAA. HIPAA requires “reasonable and appropriate safeguards” whenever e-mailing Protected Health Information (PHI), but ongoing studies show that healthcare organizations are still in the early stages of adopting effective methods to ensure private information is not transmitted in plain text.

There are substantial risks that some e-mail messages will be sent to or received by the wrong individual, read by unauthorized individuals such as the recipient’s employer or coworkers, family, friends, or intercepted in transmission by an unknown third party. Under HIPAA, organizations are required to take reasonable steps to reduce the risks. But it’s also a matter of good business practice to keep confidential information private.

These studies show many healthcare organizations still expose themselves to the significant risks posed by unprotected e-mail — even with e-mail privacy policies in place. There is a strong possibility that organizations may have a false sense of security about how effective their e-mail privacy policies are, and thus may not realize the full extent of their company’s PHI exposure.

### PHI Leaks Common

Since April 2003, the deadline for the HIPAA Privacy Rule, Zix Corporation (a partner of FORTRESS Network Security) has sampled over 12 million e-mails sent from or received by more than 7,500 healthcare organizations. Organizations whose e-mail was analyzed included health insurance plans, hospitals, physician practices, intermediaries and other healthcare-related organizations. The samples collected represent the inbound and outbound e-mail traffic for a period of three to seven days for each of the organizations that commissioned audits using an assessment tool that specifically scans for PHI. Messages that did not contain PHI, or were encrypted as a safeguard so that PHI was unreadable, were categorized as not posing a HIPAA risk.

Ninety-eight percent of all the organizations examined had unsecured PHI in their e-mail. The ubiquitous nature of e-mail makes it an easy and fast communication tool. It’s not surprising that organizations have this kind of exposure given the universality of e-mail and the convenience it supplies in day-to-day operations.

For each of the organizations studied, the average exposure rate in outbound e-mail flow was four percent. Though the number may seem low, here’s the reality: Even a small-to-medium sized healthcare organization may send as many as 5,000 messages per week. At the average four percent exposure rate, that’s 200 occurrences of unsecured PHI leaving the organization per week – or 10,000 occurrences per year.

Remember that e-mail is a high-volume channel, so even small percentages of unsecured PHI can quickly mount to a large risk. While it may be possible to send an occasional unsecured e-mail in response to specific circumstances without creating much risk, any routine or reasonably high-volume use of e-mail will create serious risks. The greater the volume of e-mail, the higher the risk, and the more evidence is available against the organization in case of a penalty action.

## **What e-PHI Looks Like**

What does this PHI look like? Manual examination of the 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 e-mail 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 payers discussing individual claims, correcting coding issues, clarifying dates, etc.

The messages also show the industry trend toward the availability of online medical information. More people use the Internet and e-mail as an integral part of daily life. As such, patients communicate with care providers via e-mail (and vice versa) asking questions, clarifying a medication, managing disease, scheduling appointments, and other things of this nature.

Appendix A illustrates two examples of e-mail messages containing PHI. Example #1 is clearly understood and easily fits HIPAA's definition of PHI. It contains a patient's social security number, medication, and diagnosis discussion. Example #2 is more common to what is seen in e-mail containing PHI. It is cryptic, full of strange abbreviations, sentence fragments and misspellings. Building tools that scan for PHI in e-mail can be challenging because of these kinds of messages. It speaks to the nature of e-mail as a communication method. It's free, open text. Regardless of the cryptic nature of the second example, both messages contain PHI and should be protected under HIPAA.

## **Finding the e-PHI Leaks in Your Organization**

Short of playing "Cyber Cop" for an organization and manually policing all outbound e-mail for PHI, how can one determine the risks – if any – that this electronic communication medium poses for said organization? The simplest and most effective method of determining one's risk of PHI transmission is to conduct an automated assessment, similar to the aforementioned studies conducted by Zix Corporation.

With various legislative acts such as HIPAA looming over organizations, many technology companies have created tools to assist with this type of process. The best providers have fashioned customized templates or lexicons to meet the exact compliancy requirements of the organization requesting the assessment. For example, a good HIPAA template should be able to infer what constitutes a leak of PHI. The template would recognize that it is okay to share Jane Doe's name, but the combination of name and diagnosis (or prescription, or case number, or even social security number) or any other combination of linkable information sets would be in violation of HIPAA privacy and security rules.

In a typical assessment, a device will be placed in the organization's network. This device will use the appropriate templates to "scan" all e-mail – including subject, body, AND attachments – as it is sent out. One should plan to collect at least 3-5 days worth of data in order to gauge real day-to-day e-mail usage. The device should work invisibly and should collect data on the sender and recipient of each message, as well as any PHI violations contained within the message (ideally this assessment device will retain a carbon copy of the message for later manual analysis). At the end of the assessment period, a report of the tool's findings should be created and reviewed by appropriate management parties.

## **Conclusion**

As you know, part of the HIPAA Security Rule has added the concept of addressable specifications to avoid strapping the law to any particular technology and to acknowledge that there are often many technical ways to accomplish the same goal. In the case of e-mail, however, an organization's options are limited by the fact that e-mail must travel across the public network. In this case, the only options are simply to encrypt the messages or block e-mail use altogether. There really is no other equivalent alternative. Either secure the mail when sending, or don't send it. The results and analysis of a proper e-mail assessment can prove invaluable to an organization when looking at such electronic communications as an "addressable" item. If your organization depends upon e-mail to communicate or conduct business, an assessment of your e-mail systems should be strongly considered.

## Appendix A

### EXAMPLE #1

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

Linda,  
Here's the info you requested on patient Jane Doe, SS# 999-99-9999.

She sees Dr. A. at General Hospital. She began tamoxifen approximately 5/15/2002.

When he saw her in 2003, he stated that she had been on Tamoxifen for a year. Her last visit was 10/14/2003. No sign of cancer.

### EXAMPLE #2

From: John@sender.net  
To: Bob@recipient.net  
Subject: Jane Doe

Hello, could you chk on this claim, member number 12345.

Dollar amt of claim is for 1283.15, dates of svc frojm 0130003 through 051603.

Patient seen at General. Sent appeal on 080603 with prime pymt, did you receive, is this in process, i emailed once, no response?

*Special thanks to Eddy Smith, ZixCorp Research Engineer, for his input and assistance in putting together this month's piece. Smith joined ZixCorp in 2001 and has held several positions related to the regulatory requirements. In January of 2003, Eddy assumed the title of research engineer and was a founding member of the ZixResearch Center™ where he leads ZixCorp's efforts in content scanning and lexicon development that enable ZixCorp's solutions to assist companies in achieving regulatory compliance.*

*FORTRESS Network Security provides a number of products and services that Covered Entities can use to ensure their compliance with HIPAA while using Internet e-mail. These solutions meet the Security Rule requirements, and include other features that support HIPAA compliance by Covered Entities. If you would like more information on e-mail assessment and auditing tools, we invite you to join us and Zix Corporation for an upcoming informational webinar. To learn more about this exclusive session for readers of the HIPAA Security Tips Newsletter, please check out the other links in this month's issue or register here: [http://www.zixcorp.com/partner\\_events/fortress.php](http://www.zixcorp.com/partner_events/fortress.php).*