zixcorp | *Email Encryption*

The Case for Email Encryption

Improve Compliance and Protect PHI on the Move

ZixDirectory

The *ZixDirectory*® includes:

- Tens of millions of members and growing at approximately 100,000 new members every week
- Nearly 1 in 5, or 1,200, U.S. hospitals
- More than 30 Blue Cross Blue Shield organizations
- Health insurers protecting data for more than 70 million people

Healthcare organizations face an ongoing compliance burden involving the protection of sensitive patient data. The task of safeguarding data grows increasingly complex as the enterprise environment adapts to demands for greater mobility support. Sensitive patient data used to simply reside on desktops. Now, the information is on the move via email and, in email, is likely being viewed on tablets and smartphones.

Strengthening Regulations

The task of achieving compliance, while always important, has added urgency in 2012 as the industry anxiously anticipates greater enforcement of the HITECH security and privacy rules. The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule provides federal protections for protected health information (PHI) held by covered entities and gives patients an array of rights with respect to that information[1]. In 2009, HIPAA was strengthened through the Health Information Technology for Economic and Clinical Health (HITECH) Act[2], calling for greater protection of sensitive personal health data. Passed as part of the American Recovery and Reinvestment Act of 2009[3], the HITECH Act sets the standard that PHI should be rendered "unusable, unreadable, or indecipherable to unauthorized users."[2]

Under the breach notification rule[4], if a breach of unsecured PHI occurs, the HITECH Act requires that covered entities and their business associates provide notification of the breach to affected individuals and the HHS Secretary. If a breach affects 500 individuals or more, the breach is published on the OCR breach list and media outlets serving the affected individuals' state or jurisdiction must be notified.

1 The Health Insurance Portability and Accountability Act (HIPAA)
http://www.hhs.gov/ocr/privacy/hipaa/understanding

2 The Health Information Technology for Economic and Clinical Health (HITECH) Act
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf

3 The American Recovery and Reinvestment Act of 2009
http://www.evendon.net/PublicService/cgi-bin/HandOff-1_0.cgi?RecoveryBill1+RecoveryBill3+0117

4 The Breach Notification Rule, section 13402 of the HITECH Act
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

"It is fair to say that this breach notification provision has been the HITECH change that has had the most extensive impact on the health care industry to date," said Kirk Nahra, a partner with Wiley Rein LLP in Washington. "Large and small breaches are being reported by the thousands. Many of these notices are leading to litigation, widespread publicity, and extensive cost."[5]

Under the new legislation, healthcare organizations that violate rules to protect patient privacy face onerous resolution agreements or possibly fines of up to $1.5 million — a considerable increase from the previous $25,000 fine. They also bear the costs of notification, consumer protection and potential lawsuits. The result is a price tag of $7.2 million per data breach, or $214 per compromised record, according to a Ponemon Institute study[6].

Top Source of Data Loss

So how does your healthcare organization protect its patient data, meet compliance standards and prevent breach costs? In assessing vulnerabilities, one potential threat rises to the top — email.

The Radicati Group estimated business users sent 41 email messages and received 100 email messages per day in 2011[7]. Further demonstrating the importance of email, Osterman Research found the average user spends 146 minutes per day in email. It has also become a popular file-transfer method, with Osterman Research estimating 20-25 percent of all email messages contain attachments[8].

With the convenience of email as a communication and file-transfer method, it's easy for users to overlook the risks; however, IT security and compliance professionals recognize changing and new threats associated with this essential business tool.

5 "The Top Health Care Privacy Issues to Watch in 2012" by Kirk Nahra, *BNA's Health Law Reporter*, December 15, 2011. http://www.wileyrein.com/resources/documents/2012%20Health%20Care%20Privacy%20Issues.pdf

6 "Assessing the Cost of Data Breach" by Jennifer Lawinski, *Baseline*, March 22, 2011. http://www.baselinemag.com/c/a/Intelligence/Assessing-the-Costs-of-Data-Breaches-108265/

7 "Survey: Corporate Email, 2011-2012" by The Radicati Group, September 2011. http://www.radicati.com/wp/wp-content/uploads/2011/09/Survey-Corporate-Email-2011-2012-Executive-Summary.pdf

8 "Educating Decision Makers about the Need for Encryption" by Osterman Research, August 2010. http://zixcorp.com/documents/white-papers/OR-Educating_Decision_Makers_About_the_Need_for_Encryption.pdf

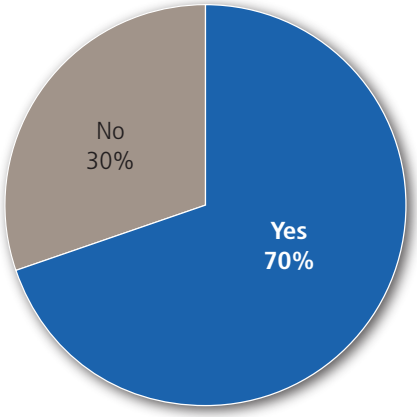
Employee Behavior - An Old Risk That Continues to Threaten

Healthcare organizations implement policies and offer employee training to prevent employees from leaking PHI, but a Ponemon Institute study[9] found this method to be insufficient. Of healthcare respondents surveyed:

- 70 percent believe employees ignore policies about emailing unencrypted sensitive or confidential documents through insecure channels
- 67 percent believe employees send unencrypted confidential information through insecure email channels, such as personal Web-based email

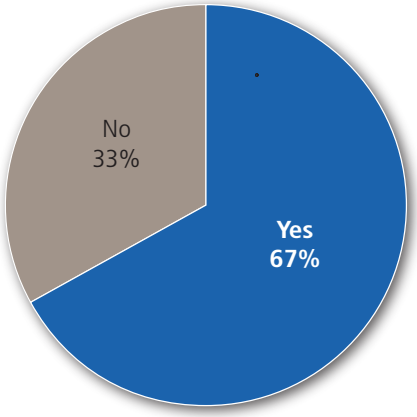
Value of Encryption Policies

Do you believe employees ignore policies about emailing unencrypted sensitive or confidential documents through insecure channels?



Use of Insecure Channels

Do you believe employees send unencrypted confidential information through insecure communication channels, such as personal Web-based email?



Malicious intent may not be common when employees circumvent company policies, but the risk of unsecure email remains the same.

"Email is essential to business productivity and collaboration. It is such a significant tool that employees are inclined to circumvent policy and email sensitive information, so they can effectively perform their responsibilities in a timely manner," said Dr. Larry Ponemon, Chairman and Founder of Ponemon Institute[10].

9 "The State of Email Encryption" by Ponemon Institute, September 2011.
http://survey.zixcorp.com

10 "Zix Corporation and Ponemon Institute Survey Reveals Risk and Frustration with Outdated Email Encryption Solutions" by Zix Corporation, September 20, 2011.
http://investor.zixcorp.com/phoenix.zhtml?c=108645&p=irol-newsArticle&ID=1608271&highlight

Mobility — A New Risk on the Rise

Business is no longer conducted behind a desk. Mobile phones have expanded the workplace and work hours, and more users spend time on email than any other internet-enabled activity. According to a study conducted by The Nielsen Company, users spend an average of 42 percent of their mobile time using email. The next most used internet-enabled activity falls to social media at 11 percent, and all other activities are under 5 percent[11].

With increasing dependence on mobile devices for access to data whenever, wherever, mobile email is a major concern. Of healthcare respondents in the Ponemon Institute study, 71 percent stated concern about the loss of information via email on mobile devices[9].

Business Associates – Expanding Accountability

With the passage of the HITECH Act, the scope of accountability for data breaches was widened beyond the covered entity to business associates (BA). New requirements under section 13401[2] apply civil and criminal penalties to BA breach violations, and covered entities are responsible for incorporating additional BA requirements in their contract agreements.

According to a *HealthcareInfoSecurity* report[12], more than 20 percent of reported breaches involve BAs. The report also revealed 24 percent of surveyed respondents perceived inadequate BA security as the biggest security threat to their organization.

To reduce breaches associated with BAs and increase confidence, secure communication and education among your BAs are critical components to any compliance strategy.

2 The Health Information Technology for Economic and Clinical Health (HITECH) Act
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf

9 "The State of Email Encryption" by Ponemon Institute, September 2011.
http://survey.zixcorp.com

11 "How Americans Spend Mobile Internet Time: A New Look" by The Nielsen Company, May 2010.
http://blog.nielsen.com/nielsenwire/online_mobile/how-americans-spend-mobile-internet-time-a-new-look/

12 "Healthcare Information Security Today" by *HealthcareInfoSecurity*, November 7, 2011.
http://www.healthcareinfosecurity.com/articles.php?art_id=4198

About Zix Corporation

Zix Corporation (ZixCorp) provides the only email encryption services designed with your most important relationships in mind. The most influential companies and government organizations use the proven *ZixCorp*® Email Encryption Services, including WellPoint, the SEC and more than 1,200 hospitals and 1,600 financial institutions. ZixCorp Email Encryption Services are powered by *ZixDirectory*®, the largest email encryption community in the world. The tens of millions of ZixDirectory members can feel secure knowing their most important relationships are protected.

For more information about ZixCorp, call 866.257.4949, email sales@zixcorp.com or visit www.zixcorp.com.

Finding Solutions and Safe Harbor in Encryption

Despite these challenges, a convenient solution is available for the protection of email — encryption.

Encryption delivers a safe harbor under the HITECH Act. As listed by the *Federal Registrar*, "While covered entities and business associates are not required to follow the guidance, the specified technologies and methodologies, if used, create the functional equivalent of a safe harbor."[13]

Combining encryption with other advances — automated, policy-based services, easy-to-use functionality and next generation mobility — address risks, concerns and compliance standards associated with email.

In preventing email data breaches with encryption, healthcare organizations secure PHI, reduce the chances for regulatory fines and decrease breach class action lawsuits. As discussed in a *HealthcareInfoSecurity* article[14], class action suits are one more reason to protect data.

"Whether or not a class action suit is successful, defending such a suit represents a significant drain of time and money and ensures unwelcome headlines. Additionally, if one of these suits succeeded in court, the damages could be staggering and the precedent could have a huge impact across the industry," said Adam Greene, a partner at the Washington law firm Davis Wright Tremaine who formerly worked at the Department of Health and Human Services' Office for Civil Rights, which enforces HIPAA[14].

Compliance is Number One

No matter the consequences of data loss — regulatory fines, breach costs, class action lawsuits — one thing is certain: compliance is the ultimate goal. In a survey[12] conducted by *HealthcareInfoSecurity*, healthcare respondents listed improving regulatory compliance as their number one information security priority for 2012. For healthcare organizations to be successful, email encryption is an essential component.

12 "Healthcare Information Security Today" by *HealthcareInfoSecurity*, November 7, 2011.
http://www.healthcareinfosecurity.com/articles.php?art_id=4198

13 HHS 45 CFR Parts 160 and 164, *Federal Register*, April 27, 2009.
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf

14 "More Breach Class Action Lawsuits Filed" by Howard Anderson, *HealthcareInfoSecurity*, November 28, 2011.
http://www.govinfosecurity.com/articles.php?art_id=4275

Zix Corporation
2711 N. Haskell Ave.
Suite 2300, LB 36
Dallas, TX 75204

866 257 4949
sales@zixcorp.com
www.zixcorp.com