zixcorp | *Email Encryption*

The Case for Email Encryption

Under the new HIPAA, PHI must be protected

ZixDirectory

The *ZixDirectory*℠ includes:

- Tens of millions of members and growing at an average of approximately 100,000 new recipients every week
- The FFIEC federal banking regulators and the Securities and Exchange Commission
- More than 20 state bank regulators
- More than 1,300 U.S. financial institutions
- Health insurers protecting data for more than 70 million people
- Nearly 1 in 5, or 1,200, U.S. hospitals
- More than 30 Blue Cross Blue Shield organizations

The revamped Heath Insurance Portability and Accountability Act (HIPAA) makes it very clear — if you're a health care organization and you don't rigorously protect your patients' personal health information, you will pay dearly.

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 protected health information (PHI) to be rendered unreadable and unusable.[1] Experts agree that encryption is a logical and easy way to protect information in transit, like email.

Tough new law has teeth

Under the new legislation, organizations can be fined up to $1.5 million dollars — up from $25,000 — for violating the rules protecting patients' privacy.[2] Their business associates are also on the hook if they're guilty of a data breach.[3] The penalties are no mere slap on the wrist — enforcement will be wide-sweeping and rigorous. State attorneys general have clear and explicit authority to enforce HIPAA's rules.[4]

Every indication shows they're ready to take HIPAA data breach violations seriously. Connecticut's Attorney General, Richard Blumenthal, filed suit against Health Net for a data breach jeopardizing the PHI of 446,000 of its members.[5] It's the first case of a state attorney general enforcing general HIPAA regulations under HITECH.[6]

1 http://www.evendon.net/PublicService/cgi-bin/HandOff-1_0.cgi?RecoveryBill1+RecoveryBill3+0117

2 Healthcare IT News, November 2, 2009 -- HIPAA violators could face fines of up to $1.5M: http://www.healthcareitnews.com/news/hipaa-violators-could-face-fines-15m

3 IT Business Edge, December 8, 2009 -- Business Associates of HIPAA-Covered Entities Need Action Plans for New Federal Breach Notification Requirements: http://www.itbusinessedge.com/cm/community/features/guestopinions/blog/businessassociates-of-hipaa-covered-entities-need-action-plans-for-new-federal-breach-notificationrequirements/?cs=37991

4 National Association of Attorneys General -- Amendments to Health Privacy Law Grant States Enforcement Powers: http://www.naag.org/amendments-to-health-privacy-law-grant-states-enforcement-powers.php

5 Connecticut Attorney General's Office, January 13, 2010 -- Attorney General Sues Health Net For Massive Security Breach Involving Private Medical Records And Financial Information On 446,000 Enrollees: http://www.ct.gov/ag/cwp/view.asp?Q=453916&A=3869

6 Fierce Healthcare, January 14, 2010 -- Health Net data breach brings first HITECH state enforcement action: http://www.fiercehealthcare.com/story/loss-info-insurance-enrollees-leads-historic-lawsuit/2010-01-14

Blumenthal said the breach exposed Health Net of Connecticut members "to grave embarrassment and emotional distress, as well as financial harm and identity theft" and that the data loss and the organization's "deliberate delay in disclosure, are legally actionable and ethically unacceptable."[7]

Ignoring the law means high fines and bad P.R.

Email is a high-volume communications channel. Even a small percentage of unsecured PHI quickly mounts to a large risk. 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.

But is this message getting through? In a 2008 security survey[8] for the Healthcare Information and Management Systems Society (HIMSS), sponsored by Booz Allen Hamilton, little more than half of those polled said they were encrypting email. In 2009, a follow-up study for HIMSS conducted by Symantec showed only a small increase in the number that bothered to encrypt data in motion—perplexing, given the enhanced enforcement and stiffer penalties meted out under the new HIPAA laws.[9]

Not encrypting sensitive data in email is a license for trouble. If an organization is caught breaking the new rules, it will face heavy penalties from both a monetary and public relations perspective. "With the theft and loss of so much information, this is a situation in which there are potentially financial and other damages in the picture. This is a public relations issue, and so much has gone on that I don't see how a provider could avoid penalties or a civil law claim," said Jud DeLoss, Chair of the Health Information and Technology Practice Group of the American Health Lawyers Association in an interview with *AIS Health*.[10]

Quite simply, if health care organizations and their business partners don't encrypt email with PHI, they face huge fines, media scrutiny, and public and government censure.

7 Insurance & Financial Advisor, January 15, 2010 -- Conn. AG sues Health Net over 'ethically unacceptable' data breach:
http://ifawebnews.com/2010/01/15/conn-ag-sues-health-net-over-ethically-unacceptable-data-breach/

8 2008 HIMSS Security Survey(Sponsored by Booz Allen Hamilton) – October 28, 2008:
http://www.himss.org/content/files/HIMSS2008SecuritySurveyReport.pdf

9 2009 HIMSS Security Survey (Sponsored by Symantec) – November 3, 2009:
http://www.himss.org/content/files/HIMSS2009SecuritySurveyReport.pdf

10 AIS Health, July17, 2009 -- The Encryption of Patient Health Records Is Crucial With New Laws and Growing Patient Desire to E-mail Their Physicians:
http://www.aishealth.com/Bnow/hbd071709.html

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, Humana, the SEC and more than 1,200 hospitals and 1,300 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.

"There is a significant risk associated with not securing data from both a regulatory and legal perspective," said Chris Apgar, President of Apgar and Associates, an information security consulting firm. "The bottom line is there is no excuse anymore for not encrypting PHI."[11]

Business associates must also protect data

It's not just health care organizations that must protect PHI but also any business associates working with them. Covered entities must still enter into written agreements with business associates. In addition, as of February 2010, business associates are subject to direct federal regulation, including civil and criminal penalties for violating HIPAA standards.[12]

"Business associates need to act quickly to take steps to minimize the risk that they will be involved in a breach that triggers these new notification requirements, and also must be prepared to respond to any breach in compliance with the HITECH Act," said Jacqueline Klosek, Senior Counsel with Goodwin Procter LLP in New York in a column in *IT Business Edge*.[13] "They can reduce the odds they'll be involved in a reportable breach by, to the extent possible, encrypting all protected health information."

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

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

7 Insurance & Financial Advisor, January 15, 2010 -- Conn. AG sues Health Net over 'ethically unacceptable' data breach: http://ifawebnews.com/2010/01/15/conn-ag-sues-health-net-over-ethically-unacceptable-data-breach/

8 2008 HIMSS Security Survey(Sponsored by Booz Allen Hamilton) – October 28, 2008: http://www.himss.org/content/files/HIMSS2008SecuritySurveyReport.pdf

9 2009 HIMSS Security Survey (Sponsored by Symantec) – November 3, 2009: http://www.himss.org/content/files/HIMSS2009SecuritySurveyReport.pdf

10 AIS Health, July17, 2009 -- The Encryption of Patient Health Records Is Crucial With New Laws and Growing Patient Desire to E-mail Their Physicians: http://www.aishealth.com/Bnow/hbd071709.html