



# The Case for Email Encryption

## Under the new HIPAA, PHI must be protected

The revamped Health 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.<sup>1</sup> 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.<sup>2</sup> Their business associates are also on the hook if they're guilty of a data breach.<sup>3</sup> 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.<sup>4</sup>

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.<sup>5</sup> It's the first case of a state attorney general enforcing general HIPAA regulations under HITECH.<sup>6</sup>

## ZixDirectory Includes

- Over 15 million protected email addresses and growing at 100,000 new recipients every week
- The FFIEC federal banking regulators and the Securities and Exchange Commission
- Over 20 state bank regulators
- More than 800 financial institutions
- 3 out of the 5 largest US health insurance companies
- More than 1,000 hospitals in the US (1 in every 7)
- Over 30 Blue Cross Blue Shield Institutions

## News Alerts:

- ZixCorp's ZixVPM 3.3 voted *Network Products Guide's* 2008 Reader Trust Award Winner for Best in Secure Email
- Positioned in the Leader's Quadrant in Gartner's *Magic Quadrant for Email Encryption*

<sup>1</sup> [http://www.evendon.net/PublicService/cgi-bin/HandOff-1\\_0.cgi?RecoveryBill1+RecoveryBill3+0117](http://www.evendon.net/PublicService/cgi-bin/HandOff-1_0.cgi?RecoveryBill1+RecoveryBill3+0117)

<sup>2</sup> 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>

<sup>3</sup> 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/business-associates-of-hipaa-covered-entities-need-action-plans-for-new-federal-breach-notification-requirements/?cs=37991>

<sup>4</sup> 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>

<sup>5</sup> 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>

<sup>6</sup> 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.”<sup>7</sup>

### **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<sup>8</sup> 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 e-mails. 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.<sup>9</sup>

Not encrypting sensitive data in emails 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*.<sup>10</sup>

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

<sup>7</sup> Insurance & Financial Advisor, January 15, 2010 -- Conn. AG sues Health Net over ‘ethically unacceptable’ data breach:

<http://faweabnews.com/2010/01/15/conn-ag-sues-health-net-over-ethically-unacceptable-data-breach/>

<sup>8</sup> 2008 HIMSS Security Survey (Sponsored by Booz Allen Hamilton) – October 28, 2008:

<http://www.himss.org/content/files/HIMSS2008SecuritySurveyReport.pdf>

<sup>9</sup> 2009 HIMSS Security Survey (Sponsored by Symantec) – November 3, 2009:

<http://www.himss.org/content/files/HIMSS2009SecuritySurveyReport.pdf>

<sup>10</sup> AIS Health, July 17, 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>

“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.”<sup>11</sup>

### 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.<sup>12</sup>

“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*.<sup>13</sup> “They can reduce the odds they'll be involved in a reportable breach by, to the extent possible, encrypting all protected health information.”

### ABOUT ZIXCORP

ZixCorp provides easy-to-use-and-deploy email encryption and e-prescribing services that protect, manage and deliver sensitive information to the healthcare, finance, insurance and government industries. ZixCorp's hosted Email Encryption Service enables policy-driven email security, content filtering and send-to-anyone capability. Its PocketScript e-prescribing service provides point-of-care access and transmission of patient and payor data that improves patient care, reduces costs and improves efficiency.

For more information about ZixCorp call toll free **866-257-4949**, email [sales@zixcorp.com](mailto:sales@zixcorp.com) or visit [www.zixcorp.com](http://www.zixcorp.com).

<sup>11</sup> *ibid.*

Dechert LLP, February 26, 2009 – Health Care Reform Update: HIPAA is Expanded to

<sup>12</sup> Cover Business Associates:

[http://www.dechert.com/library/hru\\_02-26-09.pdf](http://www.dechert.com/library/hru_02-26-09.pdf)

IT Business Edge, December 8, 2009 -- Business Associates of HIPAA-Covered Entities Need Action Plans for New Federal Breach Notification Requirements:

<sup>13</sup> <http://www.itbusinessedge.com/cm/community/features/guestopinions/blog/business-associates-of-hipaa-covered-entities-need-action-plans-for-new-federal-breach-notification-requirements/?cs=37991>