



The Case for Email Encryption

Required by Law



The ZixDirectory® includes:

- Tens of millions of members and growing at approximately 100,000 new members every week
- The FFIEC federal banking regulators and the Securities and Exchange Commission
- More than 20 state bank regulators
- More than 1,600 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

Securing sensitive personal information for customers, partners and employees isn't just a best practice — it's often the law. Compliance with regulations is a priority for healthcare, financial services and government organizations; it may also need to be a priority for your organization. Even if your organization doesn't fall directly under those industries, doesn't mean you're in the clear.

Here's an overview of federal and state regulations that you should be aware of and how email encryption is a solution for your organization's compliance.

Federal Industry Regulations

The Gramm-Leach-Bliley Act (GLBA)

GLBA¹ protects consumers' personal financial information held by financial institutions. Its "Safeguards Rule" requires all financial institutions to design, implement and maintain safeguards to secure confidential data. Its guidelines address standards for developing and implementing administrative, technical and physical processes to protect the security, confidentiality and integrity of customer information.

The Federal Financial Institutions Examination Council (FFIEC) released a handbook² on information security practices. Regarding encryption, it stated that financial institutions should use encryption to mitigate the use of disclosure or alteration of sensitive information in storage and transit³. Encryption should include:

- Sufficient encryption strength to protect the information from disclosure until such time as disclosure poses no material risk
- Effective key management practices
- Robust reliability
- Appropriate protection of the encrypted communication's endpoints

¹ "Privacy Act Issues Under Gramm-Leach-Bliley"

<http://www.fdic.gov/consumers/consumer/alerts/glba.html>

² "FFIEC IT Examination Handbook Infobase"

<http://ithandbook.ffiec.gov>

³ Encryption under the "FFIEC IT Examination Handbook Infobase"

<http://ithandbook.ffiec.gov/it-booklets/information-security/security-controls-implementation/encryption.aspx>

The Health Insurance Portability and Accountability Act (HIPAA)

The 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 information⁴.

The Health Information Technology for Economic and Clinical Health (HITECH) Act

Strengthening HIPAA, the HITECH Act⁵ calls for greater protection of sensitive personal health data. Passed as part of the American Recovery and Reinvestment Act of 2009⁶, the HITECH Privacy Rule sets the standard that PHI should be rendered “unusable, unreadable, or indecipherable to unauthorized users.”⁵

Under the HITECH Act’s breach notification rule⁷, if a breach of unsecured PHI occurs, covered entities and their business associates are required to 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.

“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.”⁸

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 fine⁵.

4 The Health Insurance Portability and Accountability Act (HIPAA)

<http://www.hhs.gov/ocr/privacy/hipaa/understanding>

5 The Health Information Technology for Economic and Clinical Health (HITECH) Act

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf>

6 The American Recovery and Reinvestment Act of 2009

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

7 The Breach Notification Rule, section 13402 of the HITECH Act

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html>

8 “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>

State Regulations

Massachusetts

Under Mass 201 CMS 17⁹, Massachusetts requires companies to encrypt all personal information of state residents transmitted electronically or wirelessly. Effective January 1, 2010, this includes Social Security and employer identification numbers, drivers' license or identity card data, account, credit and debit card numbers with any password or security and access codes. The law applies to companies within Massachusetts, as well as companies in other states that manage personal information of Massachusetts residents.

Nevada

NRS 603A¹⁰ passed in October 2008 and mandates that all businesses, no matter how small or what they do, must secure confidential customer information if it is sent electronically. Statute 603A.215 states that any form of Internet communication, including via Web sites and email, must encrypt personal data.

Washington

Passed in January 2008, HB 2574¹¹ protects personal information that is managed by any person or organization that conducts business in the state.

If personal information — including name combined with Social Security number, driver's license number, financial account information — is transmitted or stored on the internet, the law requires it to be secured and deems encryption as the accepted practice.

⁹ 201 CMR 17.00: Standards for the protection of personal information of residents of the commonwealth
<http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf>

¹⁰ NRS 603A – Security of Personal Information
<http://www.leg.state.nv.us/nrs/NRS-603A.html#NRS603ASec215>

¹¹ Washington HB 2574 – Requiring the encryption of certain personal information
<http://apps.leg.wa.gov/billinfo/summary.aspx?bill=2574&year=2008>

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.

The Future of Regulation

Compliance with regulatory requirements that protect sensitive personal information is an ongoing challenge. Although the laws reviewed above are the current standards, more federal and state laws are under consideration, including a national breach notification law¹².

Following 2011 – the year of the hack – cybersecurity is a hot topic and will continue to develop steam as a top priority. Be aware of your obligations, as well as the benefits of protecting the number one business communication tool – email.

¹² "White House Seeks National Data-Breach Notification Law" by Elizabeth Montalbano, *InformationWeek*, May 13, 2011.

<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84>

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

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