

Email Compliance Quick Reference Guide

*Strategies for Regulatory Compliance
and Legal Risk Management*

BY MICHAEL R. OVERLY

A MESSAGING NEWS PRESS PUBLICATION

Table of Contents

Introduction	5
Compliance and the Email Lifecycle	7
Getting Specific: What's in GLB, SOX, and HIPAA?	11
Gramm-Leach-Bliley (GLB)	12
Sarbanes-Oxley (SOX)	13
Health Insurance Portability and Accountability Act (HIPAA)	14
Other Regulations	15
Policy Recommendations for Messaging Managers	16
SPECIAL SECTION: Regulatory Compliance with the IronPort C-Series	18

DISCLAIMER: The law in this area changes rapidly and is subject to differing interpretations. It is up to the reader to review the current state of the law with a qualified attorney and other professionals before relying on it. Neither the authors nor IronPort make any guarantees or warranties regarding the outcome of the uses to which this material is put. This paper is provided with the understanding that the authors and IronPort are not engaged in rendering legal or professional services to the reader.

Copyright© 2006 Messaging News Press. All rights reserved. Trademarks are property of their respective owners.

“Implementing compliance architecture with an enterprise’s current technology can help reduce the cost of regulatory compliance.”

RICH MOGULL
Director, Gartner Research

Introduction

This guide is designed as a quick reference for today’s technical managers, providing an understanding of each of these email compliance laws and regulations and the potential impact on corporate messaging.

Approaching deadlines, regulatory enforcement actions, harsh penalties, along with the prospect of enormous civil damages and even criminal prosecution have made regulatory compliance and legal risk management a top priority for email/messaging managers and CIOs. In fact, according to a recent survey by Ferris Research, regulatory compliance ranks #3 on the list of top concerns of CIOs, just behind viruses and spam.

Managers tasked with creating a regulatory compliance strategy for their organizations are confronted with an alphabet soup of new laws and regulations — SOX, HIPAA, GLB— concerning what they can and can’t do with email. These rules, as well as others, require every organization to rethink and even rebuild their messaging policies, practices, and infrastructure.

Each of these regulations is complex, and none have been written with an eye to the real capabilities of current messaging technologies, or the typical corporate practices that have evolved to meet the demands of business and other practical requirements. Fortunately, effective technical solutions for policy enforcement are now available, and there is considerable overlap in the changes to messaging policies and practices that all of these laws require.

In this guide we outline the legal requirements of some of the most important laws affecting messaging, suggest some reasonable approaches to corporate email policies, and include a special section about products and services available today from industry leader IronPort® Systems. As with any compliance-related activity, your business must consult its professionals (e.g. lawyers, accountants, and consultants) to assess the measures it must take to comply with the specific laws and regulations applicable to its activities.

“...companies must take a fresh look at email hygiene to ensure that mission-critical email systems are stable, secure, and in compliance with appropriate regulations.”

MATT CAIN
META Group

Compliance and the Email Lifecycle

To develop an effective email policy and compliance solution, it is necessary to understand the lifecycle of email communications and how it relates to specific laws, as well as technical requirements and capabilities.

The lifecycle model covers the creation, distribution, and management (including storage and eventual disposal) of email and other corporate records. It is fundamentally about process, rather than technology, and governs the world of traditional records management. It is therefore congruent with other corporate records management practices — proven over decades of experience to minimize legal risk and maximize compliance.

One of the problems that makes regulatory compliance so difficult is that email functions both as a transient communication—like a phone call—and as a permanent record—like a formal memo. While users tend to be casual in their email communications, the legal status of email messages has gradually shifted from that of messages that can be handled casually, to nearly permanent records that must be carefully maintained and administered. The lifecycle framework bridges the gap between these two modes of email use.

In summary, the lifecycle approach allows managers to develop a comprehensive strategy for regulatory compliance and risk management, and bridges the domains of law, corporate policy, and messaging technology.

The Email Lifecycle

Part 1: **Creation** Part 2: **Distribution** Part 3: **Management, Storage, and Disposal**

Part 1: Creation	Legal and Policy Requirements	Technical Approaches to Compliance
<ul style="list-style-type: none"> • Email records may originate from an organizations own personnel or from outside. 	<ul style="list-style-type: none"> • Ensuring each message originates with from a specific person (SOX). • Ensuring security measures are implemented to guard against unauthorized access to messages containing protected health information (HIPAA). • Appending appropriate disclaimers (risk reduction). For example, ensuring messages containing company trade secrets or protected health information are clearly marked as “Proprietary” or “Contains Protected Health Information” to ensure they are properly handled. • For messages originating outside the organization, there may be requirements for decryption, authentication, or inbound scanning to prevent security threats (e.g., viruses and other destructive code), hate speech, or adult content. 	<ul style="list-style-type: none"> • Unique user IDs • Signing • Encryption • Appending message disclaimers

The Email Lifecycle

Part 1: **Creation** Part 2: **Distribution** Part 3: **Management, Storage, and Disposal**

Part 2: Distribution	Legal and Policy Requirements	Technical Approaches to Compliance
<ul style="list-style-type: none"> • How are records transmitted inside and outside the organization? 	<ul style="list-style-type: none"> • Preventing leakage of protected health information (HIPAA) or personally identifiable, non-public financial information (GLB). • Providing audit trails of communications (SOX) and privacy practices (HIPAA, GLB). • Preventing unauthorized access to corporate trade secrets and other proprietary and confidential information. • Preventing the forwarding of sensitive messages (e.g., those containing proprietary information, attorney-client communications, or protected health or financial information) or inappropriate or adult content. 	<ul style="list-style-type: none"> • Outbound content filtering of messages for both corporate proprietary information, protected data, and adult content. • Reputation management • Logging • Reporting

The Email Lifecycle

Part 1: Creation Part 2: Distribution **Part 3: Management, Storage, and Disposal**

Part 3: Management, Storage, and Disposal	Legal and Policy Requirements	Technical Approaches to Compliance
<ul style="list-style-type: none">• How are records managed, stored, and deleted?	<ul style="list-style-type: none">• Ensuring relevant stored messages can't be accessed or altered by unauthorized parties (HIPAA, GLB).• Ensuring messages can be retrieved as needed (SOX, HIPAA, risk management)• Proving compliance with confidentiality requirements with reports on access to message archives. (SOX)• Ensuring messages are retained as required. For example, in the event of litigation or a regulatory audit, a business will be under a duty to ensure messages are preserved and not deleted during the pendency of the proceedings. As such, businesses should develop business and technical procedures to ensure preservation of relevant messages.	<ul style="list-style-type: none">• Secure storage• Indexing• Logging• Reporting• Archiving• Secure deletion

Note: As email records are created, shared, and managed, different legal requirements come into play, and different technical capabilities are required.

Getting Specific: What's in GLB, SOX, and HIPAA?

Gramm-Leach-Bliley (GLB)

The Gramm-Leach-Bliley Act of 1999 (sometimes called the Financial Modernization Act, and usually known as GLB) is intended to ensure protection of consumers' private financial data, which the Act refers to as Nonpublic Personal Information (NPI). GLB applies to a wide range of financial institutions and other organizations that maintain NPI related to their customers.

The areas of greatest concern to most companies, and to corporate messaging managers, are the Financial Privacy Rule, which covers the collection, use, and disclosure of NPI, and the Safeguards Rule, which describes the processes companies must take to protect NPI.

The Financial Privacy Rule is relevant to messaging because it covers the implementation of opt-out policies and privacy notices. For the most part, these are technology independent.

The Safeguards Rule is more directly related to messaging infrastructure. It states that companies must maintain security programs that are commensurate with their size and complexity, as well as with the sensitivity of the NPI. More specifically, the Rule covers the use of technologies to prevent interception, automated enforcement of corporate policies related to message content, and general email security provisions.

While GLB doesn't make reference to specific technologies (i.e., the law is "technology neutral"), in practice, the Safeguards Rule means that companies should implement policy enforcement tools that can encrypt or block email traffic based on message sender, recipient, and content as appropriate. In addition, companies must implement systems that provide logging and reporting—allowing them to demonstrate compliance. Protection from spam, phishing, and viruses may also help demonstrate compliance, since these forms of traffic may increase the risk of unauthorized use, and pose a threat to the integrity and security of the NPI.

Sarbanes-Oxley (SOX)

The Sarbanes-Oxley Act, better known as SOX, affects only public companies, but has far broader applications than GLB and includes criminal penalties for individual executives who fail to comply with its provisions.

The intent behind SOX is to bring greater accountability and transparency to corporate financial operations. Administered primarily through the Securities and Exchange Commission, SOX currently affects all public companies, with its greatest impact presently being felt by those with a market cap greater than \$75 million.

Section 302, which assigns responsibility for financial reports, and Section 404, which describes required internal controls, are the two sections most relevant to the messaging system. Between them, these provisions include several requirements directly relevant to email policies and practices, including requirements for:

- identification and handling of information that must be kept confidential
- identification of individual message senders
- confidential transmission of email
- hardening email and other servers that store confidential information
- tracking and logging message traffic
- auditing capabilities
- message indexing, archiving, and retention

As with GLB, SOX isn't specific about the precise policies or technical means companies use to implement these requirements. However, there is no question that SOX compliance will force changes to the messaging architectures used by public companies.

In particular, the requirements for identity management (i.e., positive identification of message senders and recipients), message security and integrity, and message indexing and archiving, are not typical capabilities of today's corporate mail systems.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) places a number of requirements on the healthcare industry's information handling practices, and has a number of direct impacts on the operation of messaging systems. HIPAA is a particularly urgent matter in the healthcare industry because enforcement of the privacy rules will begin (for most organizations) on April 21, 2005.

Under HIPAA, organizations must ensure that email messages containing protected health information are secured, even when transmitted via unencrypted links, that senders and recipients are properly verified (technically, HIPAA's "person or entity authentication" standard applies only to "a person seeking access to electronic protected health information," not to the sender of that information) and authenticated, and that email servers and the messages they contain are protected. In other words, HIPAA affects both information in transit, and information at rest.

As with GLB and SOX, there are no specific references to particular technologies used to implement these rules. Rather, the rules can be seen as an attempt to mandate best practices of information security. There is a broad consensus in the technology community that technical approaches such as authentication, encryption, content filtering, hardened message server software, and archiving, as well as anti-spam and anti-virus technology, are appropriate means for meeting HIPAA requirements. This remains a dynamic area however, and the Centers for Medicare and Medicaid Services (CMS) recently announced its intent to issue additional guidance on this issue.

Other Regulations

HIPAA, GLB, and SOX are not the end of the story. Laws, regulations, and industry practices concerning email are proliferating:

- **California 1386.** Effective since July, 2003, this mandates public disclosure of computer-security breaches in which confidential information of California residents may have been compromised.
- **ISO 17799.** A generic set of best practices in information security that is rapidly gaining acceptance worldwide.
- **Family Educational Rights and Privacy Act (FERPA).** FERPA governs the privacy of student records in any medium, including email, and applies to any institution that receives funds from the Department of Education.
- **California AB 1350.** Businesses that own or license personal information about California residents must implement "reasonable security procedures" to protect that information.
- **Joint Commission on Healthcare Organizations (JCHO).** This Commission has developed information practices for healthcare organizations.

Clearly, the changing legal environment will place new and somewhat unpredictable demands on both email infrastructure and technical managers.

Policy Recommendations for Messaging Managers

Messaging managers must translate the legal requirements of GLB, SOX, HIPAA, and other applicable regulations into corporate messaging policies and practices, and then into decisions about technology requirements.

Equally important, managers need to carefully consider potential liabilities and legal risks associated with the operation of their email systems.

Given the continuous evolution of regulatory requirements, managers need to ensure that the decisions they make concerning messaging infrastructure won't lock them into dead ends or create additional risk. Furthermore, messaging infrastructure must support different requirements in different parts of the world, applied to different groups of employees, and to different types of message traffic.

In practice, this means paying close attention to several technologies and associated practices:

Identity verification and information protection. To verify the identity of both senders and recipients, and to protect confidential and proprietary information, managers need to develop and implement email encryption technology, at least for some subset of their users and communications.

Content scanning and filtering. Based on a variety of conditions—who is sending the message, who is the intended recipient, what is in the message—content filtering allows automatic enforcement of email policies. For example, HIPAA and GLB require businesses to scan outbound email messages for protected information (such as patient medical information, social security numbers, and bank account numbers) and perform specific actions on messages that contain these lexicons. Similarly, some organizations must automatically encrypt messages destined for business partners or refuse to accept unencrypted emails from senders that require secure communication.


Archiving. Under SOX and certain other laws, relevant email messages must be retained for up to seven years. In addition, message archives must be indexed and accessible—the list of firms fined by the SEC for failure to maintain adequate records is long and growing, as are the amounts of fines imposed. In 2002, the SEC fined five firms \$8.25 million for lack of compliance with email retention requirements relating to client communications; in 2004, it fined one company \$10 million for flawed recordkeeping.

Policy enforcement, monitoring and reporting. Translating corporate policies into practice requires some technical means of automated enforcement. Without monitoring, reporting, and strong auditing capabilities, there can be no enforcement, nor any proof of compliance. Any technological solution to the compliance issue must include logging and reporting capabilities. In addition, this solution must enforce strict access control rules, thereby guaranteeing that only authorized users make changes to existing policies.

Reputation and user authentication. Maintaining a good online reputation is essential to mail deliverability, and no company can expect to maintain a good reputation if many of its connected machines are zombies sending out floods of spam. While failure to prevent this from happening has yet to result in substantial damage awards, part of the intent of an email policy, and a system to enforce it, is to maintain an organization's good reputation.

Virus and spam protection. While spam and virus prevention are not directly called for in any of the major laws discussed here, they do provide protection of information, eliminate distribution of adult content, and defend against phishing and other attacks that could compromise the security and integrity of confidential and proprietary information, or create liability.

Given this set of requirements, it is not appropriate, but also necessary for messaging managers to begin assessing specific products and services.



Regulatory Compliance with
the IronPort C-Series Email
Security Appliance.

SPECIAL SECTION SPONSORED BY IRONPORT SYSTEMS

IRONPORT'S COMPLIANCE SOLUTION:

Powerful Tools Enabling Simple Management of Complex Tasks.



MAKING THE INTERNET SAFE.

FOR MESSAGING MANAGERS working to ensure regulatory compliance, IronPort's email security appliances provide a powerful and flexible infrastructure for policy enforcement. IronPort's appliances protect internal servers from attacks, and enable organizations to comply with HIPAA, GLB, SOX, and other regulatory compliance laws by applying filtering, encryption, and archiving policies on incoming and/or outgoing messages. IronPort email security appliances provide the critical tools for compliance management, including:

- **Protection of sensitive information and verification of user identity.** Industry-leading encryption technology enables IronPort users to comply with regulatory requirements related to the securing of health and financial information. IronPort's secure email delivery solution seamlessly encrypts, decrypts, and digitally signs confidential email messages. IronPort's integration with encryption partners (PGP Corporation, PostX, Sigaba, and Authentica) provides a unified solution for enforcing granular encryption policies, and guarantees message signing (sender and recipient verification) and integrity while protecting messages stored on servers.
- **Content scanning and filtering for email policy enforcement.** The IronPort content scanning engine allows organizations to effectively monitor messages for sensitive information. Pre-defined content filters for HIPAA, GLB, and other regulations automatically scan emails for protected financial and health information. Easily extensible lexicons allow companies to customize these rules to meet specific requirements. The IronPort content scanning engine filters messages based on message or attachment content, subject, sender, recipient, message headers, or message body. These capabilities allow for a wide variety of policy enforcement options—drop, bounce, alter, archive, or encrypt a message, generate a notification, or blind carbon-copy the message to an archive or a compliance officer.

- **Archiving.** To ensure messages are properly preserved, indexed, and accessible, archiving is a critical component of the vast majority of compliance programs. Through the use of open standards, and partnerships with leading vendors such as Veritas, IronPort helps users ensure email records are secured and stored properly.
- **Enterprise management tools including monitoring and reporting.** To support policy management and auditability, IronPort Mail Flow Monitor™ and Mail Flow Central™ provide complete real-time visibility into email traffic. Detailed logs and reports identify messages that trigger specific policy rules and track the actions taken on these messages. For example, an email administrator can verify whether outgoing messages to a particular recipient were encrypted. This enables administrators to effectively meet the logging and reporting requirements of even the most stringent regulatory requirements. Additionally, this information is maintained under change control, which provides the kind of auditability called for in e-mail related regulations.
- **Total Email Security.** Installed at the boundary of an organization's messaging infrastructure, the IronPort appliances are positioned to protect internal servers from attack. IronPort email security appliances utilize preventive and reactive technology to provide the highest levels of protection. IronPort Virus Outbreak Filters™ and IronPort Reputation Filter™ technologies scan inbound and outbound messages and respond immediately to spam and virus attacks. Messages that pass through this layer are scanned by industry leading anti-spam and anti-virus technologies

Taken together, these features and capabilities allow IronPort users to address the full range of requirements in each part of the email lifecycle, from message creation and distribution, to management, storage, and eventual disposal.

Unlike servers built only to transfer mail, IronPort's security appliances are built as high performance servers capable of managing complex tasks related to security and policy enforcement. By using or utilizing open

standards, and close alliances with leading vendors of archiving, encryption, anti-spam, and anti-virus products, IronPort ensures its users are provided with access to both a unified platform and integrated best-of-breed products.

Given the complexity of existing laws and regulations, and the certainty of continual change in the legal environment, it is only by adopting the most powerful and flexible email security platforms and management systems that technical managers can hope do their part in ensuring regulatory compliance and reducing the legal risks facing their organizations. More information about IronPort can be found at www.ironport.com.

ABOUT THE AUTHOR

MICHAEL R. OVERLY is a partner in the e-Business and Information Technology Group in the Los Angeles office of Foley & Lardner. As an attorney, Certified Information Systems Security Professional (CISSP), and former electrical engineer, his practice focuses on counseling clients regarding technology licensing, information security, electronic commerce, and Internet and multimedia law. Mr. Overly writes and speaks frequently on the legal issues of doing business on the Internet, technology in the workplace, e-mail, and electronic evidence. Mr. Overly has written numerous articles on these subjects and has authored chapters in several treatises. He is the author of the best selling e-policy: *How to Develop Computer, E-mail, and Internet Guidelines to Protect Your Company and Its Assets* (AMACOM 1998), *The Open Source Handbook* (Pike & Fischer 2003), *Licensing Line-by-Line* (Aspatore 2004), *Overly on Electronic Evidence* (West Publishing 2002), and *Document Retention in The Electronic Workplace* (Pike & Fischer 2001). Mr. Overly can be reached at moverly@foley.com.