appriver®
Email & Web Security Experts™

Email Compliance in 5 Steps

Introduction

For most businesses, email is a vital communication resource. Used to perform essential business functions, many organizations rely on email to send sensitive confidential information within and outside the organization. Yet the prevalence of email as a business tool also makes it vulnerable to exploitation and data loss. In fact, email accounts for 35% of all data loss incidents among enterprises According to a recent industry study. Email’s many vulnerabilities underscore the need for organizations to secure, control and track their messages and attachments wherever they send them.

For organizations subject to regulatory compliance, securing email communications has an added level of complexity and obligation.

Organizations are challenged to navigate a growing, disparate and constantly changing framework of regulations or face harsh penalties and sanctions. While it seems simple enough to relegate the heavy burden of email compliance to an out-of-the-box solution, no technology can ensure compliance alone. That's why it is essential for today's businesses to develop an effective policy of email compliance for specific regulations that are subject to and implement flexible technology solutions that enforce this policy.

While regulations governing messaging security can be complex, email security doesn't have to be.

The bad news is that there is no universal recipe, guidebook or plan that can lead all organizations to compliance. Why? Because every organization is unique.

The good news is that there are a few steps all organizations can follow that will simplify the task of developing an email compliance policy.

Step 1:

Determine What Regulations Apply to Your Organization and How to Meet Requirements for Email Compliance

What regulations apply to your organization? What requirements exist to demonstrate email compliance? Do these email compliance regulations overlap or conflict? Determine if you need different policies for different regulations or one comprehensive policy. Following are examples of major regulations affecting organizations' email encryption policy:

	Who it Affects:	**What it Requires:**
Health Insurance Portability & Accountability Act (HIPAA)	All organizations that directly maintain and transmit protected health information including hospitals, physician practices, and insurance brokers. Business partners and vendors that exchange data with such organizations are also subject.	Organizations must ensure that email messages containing personally identifiable health information are secured, even when transmitted via unencrypted links, that senders and recipients are properly verified.
Sarbanes-Oxley Act (SOX)	All public corporations, with harsher penalties for corporations with market caps in excess of $75 million. Holds corporate executives personally accountable.	It demands companies establish internal controls to accurately gather, process and report financial information. Encryption for financial information sent via email is necessary to ensure data integrity, unauthorized disclosure or loss.
Gramm-Leach-Bliley Act (GLBA)	Broad array of organizations within the financial industry. These include banks, credit unions as well as additional businesses of a financial nature.	Organizations must implement policy and technologies that ensure the security and confidentiality of customer records when transmitted and in storage.
Payment Card Information Security Standards (PCI)	Merchants and other organizations who transact using major credit, debit, and prepaid cards as well as third party payment card processors.	The secure transmission of cardholder data against interception and unauthorized disclosure as well as protections against malware and other threats to the integrity of cardholder data.

Step 2:

Identify What Types of Data Sent Via Email Require Protection and Set Protocols Accordingly

Depending upon what email compliance regulations your organization is subject to, you must identify data deemed confidential—be it credit card numbers, electronic health records, or personally identifiable information—that is being sent via email. Then your organization must determine who should have access to send and receive such information.

Step 3:

Determine If and How Data is Being Leaked or Lost

Once you understand what types of data are being transmitted via email, you can track if and how data is being lost through email. Are breaches occurring inside the organization? Within a specific group of users? Are file attachments being leaked? Set additional policies to address you core vulnerabilities.

Step 4:

Identify What Email Solutions you Need to Implement your Policy and Remain Compliant

Having the right solutions to enforce policy is just as important as the policy itself. To satisfy regulatory requirements and enforce policy, several solutions may be necessary to ensure email compliance. Below are solutions organizations can implement to enforce policy and help address technical security safeguard standards:

End-to-end encryption:

To meet regulation requirements that mandate email messages containing relevant confidential data be secured, end-to-end encryption is often necessary to ensure that data remains confidential and secure between the message sender and the intended recipient, preventing unauthorized access or loss.

Archiving:

Some regulations require that relevant email messages must be retained, indexed and remain accessible for a period of time after transmission. A proper email archiving system will enable organizations to meet regulatory requirements for message retention and auditing records by capturing, preserving and making all email traffic easily searchable for compliance auditors to evaluate. When encrypted and backed-up, archiving provides additional protections for information against loss and unauthorized exposure.

Antivirus:

Antivirus and anti-malware solutions provide additional protections against exploitation or loss, defending against phishing and other attacks at the email gateway that could compromise the security of confidential data.

When selecting an email technology solution, it is important to consider how email is functioning in your organization and implement a solution that will support business processes and current workflow. Often technologies created to enable regulatory compliance inhibit functionality and workflow, frustrating users. According to a recent study conducted by the Ponemon Institute, over half of email encryption users were frustrated with their encryption solutions being difficult to use.

Step 5:

Educate users on applicable policies for email to protect sensitive data

An effective email compliance policy focuses on user education and policy enforcement. As unintentional human error remains one of the most common causes of data breach, many regulations now require educating users on the behaviors that potentially cause breach. When users understand proper workplace email usage, the consequences of non-compliance, and become comfortable using appropriate technologies, they will be less likely to let their guard down and make mistakes.

Secure Email Shouldn’t Change Your Workflow

CipherPost Pro® is a cloud solution for email encryption, secure file transfer and DLP that helps address compliance, technical security, safeguard standards, and lets you use your email just the way it is.

Helps address HIPAA, SOX, GLBA and PCI technical security safeguard standards for secure and confidential email transmission of data.

Simplifies the complexity of secure electronic communications, integrating seamlessly with any email platform including MS Outlook, MS Office 365, Gmail and Zimbra (for both sender and recipients regardless of their network configuration).

Eliminates size limitations for secure file transfer, enabling transmission of medical scans (X-rays) and other large files.

Enables secure web forms for capturing information from directly your website such as doctor consultations via email, insurance claims, and collections.

Enables Secure e-Statements for secure and traceable invoicing. Automates and securely delivers messages and file attachments decrypted to any email archive database or third party application through a secure API.

Enables anytime, anywhere secure communication and collaboration by allowing users to send, track and receive secure email and medical files on any mobile device including iPhone, iPad, Android, BlackBerry and Windows Phone.

CipherPost Pro®

- Email can travel a long way before it hits your inbox. With CipherPost Pro® from AppRiver, you'll avoid prying eyes along the way.

- Features and benefits:
  - Secure, fast and easy to use
  - Protects confidential information and helps ensure regulatory compliance
  - Provides delivery slip and registered mail options
  - Features centralized management and reporting
  - Enables large file attachment encryption and delivery
  - One-click encryption
  - Includes Outlook plug-in, Windows and Mac desktop agents, browser plug-ins
  - Full-featured functionality for mobile devices including iPhones, iPads, BlackBerry, Windows Phone, Android and more
  - Compatible with Office 365
  - Includes Phenomenal Care® from our US-based team, 24 hours a day, every day

- AppRiver's Phenomenal Sales advisors can provide information on which features are available with CipherPost Pro email encryption service. Contact sales@appriver.com for more information.

appriver®
Email & Web Security Experts™

Learn more about **CipherPost Pro®** at www.appriver.com

About CipherPost Pro®

The makers of CipherPost Pro® believe that email security should complement your email, not complicate it. Our cloud-based solutions for secure file transfer and email encryption work seamlessly with any email to enable secure communication and collaboration anytime, anywhere.