DeliverySlip

WHITE PAPER

Five Steps to Email Compliance

Introduction

For most businesses, email is a vital communication tool. Many organizations rely upon on email as the primary method of sharing sensitive confidential information. However, the prevalence of email as a business tool also makes it vulnerable to exploitation and data loss. In fact, email accounts for a significant amount of all data loss incidents among enterprises. 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 such as HIPAA (Health Insurance Portability & Accountability Act), securing email communications can be complicated and time-consuming. 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 compliance to an out-of-the-box solution, no technology can ensure compliance alone. It becomes essential that organizations develop an effective policy for email compliance for specific regulations they are subject to, implement flexible technology solutions that enforce that policy, and ensure that those policies and standards are readily available and understandable to anyone with access to the information.

Unfortunately, there is no universal recipe, guidebook, or plan that will help organizations comply with every regulation regarding securing email communications for their industry or jurisdiction. Every organization is unique. On the bright side, there are a few steps all organizations can follow that can simplify the seemingly complex task of developing email compliance policy. While regulations governing messaging security can be complex, email security doesn't have to be. This white paper outlines five straightforward steps that organizations can follow to develop an effective policy to help address technical security safeguard standards.

1. Determine requirements based on applicable regulations

In order to develop a comprehensive strategy for email compliance, privacy, and data protection, the first step is to understand what regulations may affect your organization's email policies.

HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT (HIPAA)

WHO IT AFFECTS HIPAA impacts 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.

WHAT IT REQUIRES Organizations must ensure that email messages containing personally identifiable health information are secured. Senders and recipients must be properly verified.

SARBANES-OXLEY ACT (SOX)

WHO IT AFFECTS SOX impacts all publicly listed corporations, with penalties increasing for corporations with market caps in excess of $75 million. The Act holds corporate executives personally accountable.

WHAT IT REQUIRES SOX 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)

WHO IT AFFECTS GLBA impacts a broad array of organizations within the financial industry, including banks, credit unions, and other financial services institutions.

WHAT IT REQUIRES 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 DSS)

WHO IT AFFECTS PCI DSS impacts merchants and other organizations who transact using major credit, debit and prepaid cards, as well as third-party payment card processors.

WHAT IT REQUIRES Organizations must ensure the secure transmission of cardholder data against interception and unauthorized disclosure, as well as protections against malware and other threats to cardholder data integrity.

2. Identify what needs protecting & set protocols

Depending upon what regulation(s) your organization is subject to, identify any data deemed confidential—credit card numbers, electronic health records, or personally identifiable information—being sent via email. After determining who should have access to transmit such information, set policies that can be enforced by technologies to encrypt, archive, or even block transmission of email content, based on users, user groups, keywords, and other means of identifying transmitted data as sensitive.

3. Track data leaks & losses

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 core vulnerabilities.

4. Identify the solution you need

To satisfy regulatory requirements and enforce policy, several solutions will be necessary to ensure compliance. Below are of some the solutions that organizations should consider:

END-TO-END ENCRYPTION

To meet regulatory requirements that mandate secure transmission of email messages containing relevant confidential data, end-to-end encryption is often necessary. Encryption ensures that data remains confidential and secure between the message sender and the intended recipient, preventing unauthorized access or loss.

DATA LEAK PREVENTION (DLP)

A DLP solution for email is often essential for email compliance. DLP provides enhanced email security through content filtering, authentication, and permission rules that limit access and transmission of sensitive information sent within and outside the organization.

ARCHIVING

Some regulations require that relevant email messages 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 by compliance auditors. When encrypted and backed-up, archiving provides additional protection for information against loss and unauthorized exposure.

ANTIVIRUS

Antivirus and anti-malware solutions provide additional protection 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. Technologies created to enable regulatory compliance often frustrate users by limiting functionality and inhibiting workflow.

5. Educate your users

Employee education is a critical component of ensuring compliance, as human error remains one of the most common causes of data breaches. Many regulations require the education of users on behaviors that could potentially breach policy. Common examples include, but are not limited to, clicking on risky links, replying to spam, and storing credit card information. When users understand proper workplace email usage and the consequences of noncompliance, and are comfortable using appropriate technologies, they will be less likely to let their guard down and make mistakes.

DeliverySlip can help

In an age of growing regulatory oversight and increased pressure to safeguard customer data, DeliverySlip simplifies compliance efforts.

SECURING YOUR EMAIL SHOULDN'T CHANGE YOUR WORKFLOW

DeliverySlip is a simplified, secure, cloud-based communications and information management solution that enables companies to protect and control email and valuable company data.

More than 10,000 customers worldwide in every industry sector depend on DeliverySlip' innovative platform to communicate securely on any device, control what happens to their messages even after they have been sent, rapidly share large files, obtain legally binding e-signatures and e-approvals, and prevent unauthorized data loss.

DeliverySlip uses existing email accounts and integrates seamlessly into email clients, including Outlook, Office 365, and Gmail. There's virtually no learning curve and your users can be set up for secure communication and collaboration in minutes.

Benefits

DeliverySlip eases regulatory compliance by:

- Helping to address HIPAA, SOX, GLBA, PCI and other technical security safeguard standards for secure and confidential transmission of messages and files
- Simplifying the complexity of secure electronic communications, integrating seamlessly with email platforms (including Outlook, Office 365 & Gmail), existing Data Leak Prevention (DLP) tools, and SSO environments (including OAuth 2.0 & SAML 2.0)
- Enabling anytime, anywhere secure communication and collaboration with fully functional mobile apps for most devices, including iOS, Android, and others
- Providing real-time updates and advanced message control with features such as ReplyFreeze, True Recall, Message Expiry and setting extra password protection on individual messages
- Enabling secure sharing of large files (e.g., X-rays, blueprints, contracts) from within email, eliminating the need for any extra workflow and not exposing your data to third-party apps
- Making it simple to securely request or provide legally-binding e-signatures and e-approvals on documents and images right from an email message
- Supporting message retention requirements through integration into email archiving technology

DeliverySlip

About DeliverySlip

Powered by 10 patents and stress tests by KPMG, you can trust DeliverySlip to keep your communications safe. DeliverySlip is the leader in email encryption and file security. Used and trusted in virtually every industry with over 5 million users and growing every day.

Be Productive, Be Collaborative, Be Secure

TRY IT FREE | DELIVERYSLIP.COM OR 1.877.404.9964