HIPAA Email Compliance & Privacy

What You Need to Know Now

Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) places a number of requirements on the healthcare industry to assure that individuals' health information is properly protected while allowing the swift flow of health information needed to provide high quality health care.

As **electronic health records (EHR)** are becoming an industry standard for maintaining and transmitting health information, email emerges as the obvious choice for exchanging EHR quickly and efficiently among healthcare organizations.

But Email's Expediency Is Not Without Vulnerability…

Data can be leaked or lost through a variety of means:
from malware to phishing to user-error.

In The Case Of Healthcare Organizations

this can mean the loss or unauthorized disclosure of patient medical files or other patient information exchanged via email.

As email is the choice means for exchanging patient information, HIPAA's aim to secure patient data underscores the need for healthcare organizations to secure their email communications with HIPAA compliant email encryption.

Who Is Affected by HIPAA

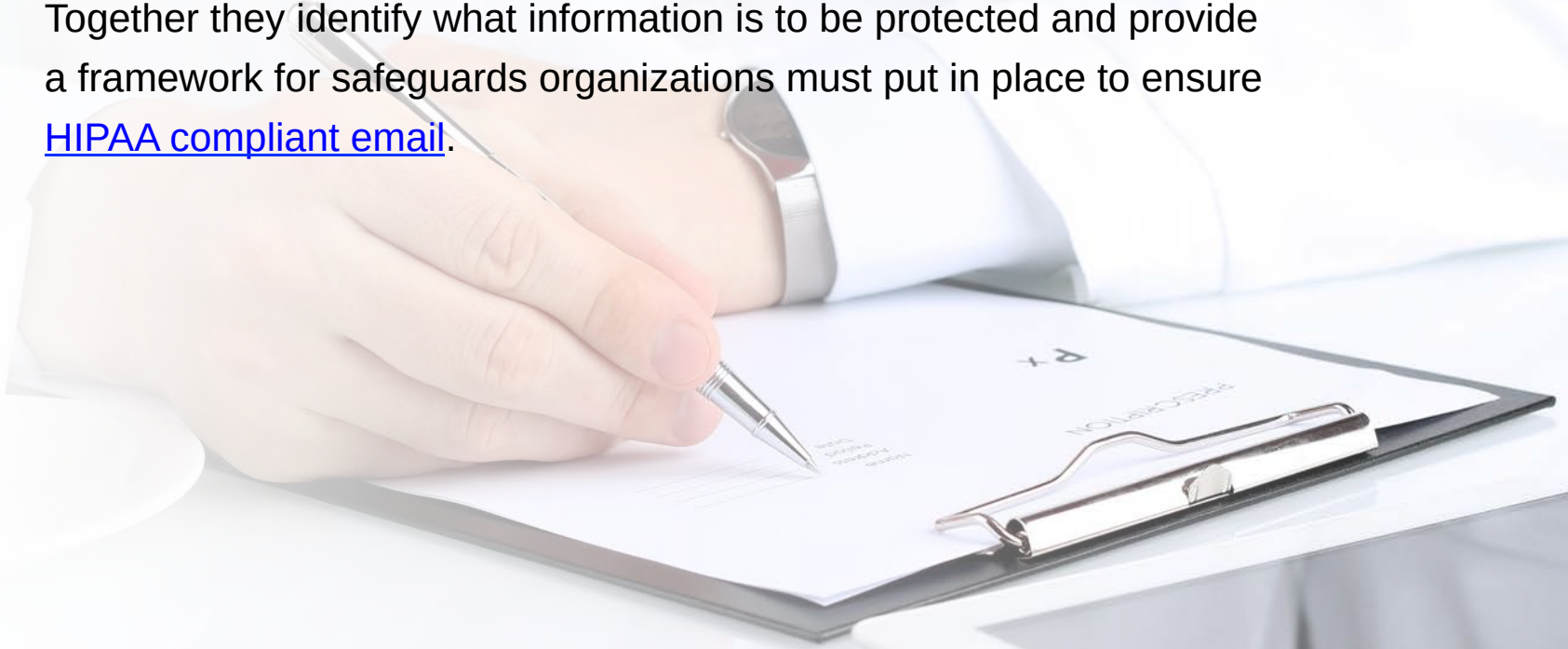
HIPAA applies to all organizations that directly maintain and transmit personally identifiable health information, referred to by HIPAA as protected health information (PHI), or e-PHI in electronic form. These include hospitals, physician and dental practices, health insurance brokers and carriers, laboratories, and pharmacies. Additionally, HIPAA applies to third party vendors and business partners that exchange data with organizations that directly maintain and transmit PHI in any form.

Why Should Healthcare Providers Care about HIPAA Compliant Email?

It's no secret that non-compliance can be costly, or even crippling to your business. Under HIPAA, healthcare organizations that fail to secure PHI against loss or unauthorized disclosure face fines of up to $250,000 per incident while individuals responsible can face up to 10 years in prison for non-compliance. In addition to harsh financial penalties and criminal proceedings, violators are required by the Department of Health and Human Services to report their compliance breaches to affected parties as well as the media if a breach affects 500 or more individuals. Without question, the ensuing legal entanglements, reputation damage and financial cost of HIPAA violations threaten your business's bottom line and may critically your organization's ability to do future business.

What are the Requirements of HIPAA Compliant Email?

Two provisions under HIPAA directly impact healthcare organizations' email policy and security: The Privacy Rule and the Security Rule. Together they identify what information is to be protected and provide a framework for safeguards organizations must put in place to ensure HIPAA compliant email.



The Privacy Rule

The Privacy rule defines what patient information is to be protected and places healthcare organizations responsible for the confidentiality of PHI in any form, including EHR. Under HIPAA, protected health information (PHI) is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

The Security Rule

Consequently, the Security Rule mandates that affected organizations implement appropriate policies, technical and physical safeguards for information systems that maintain e-PHI, including email, to ensure the security and confidentiality of e-PHI against loss or unauthorized disclosure.

Specifically HIPAA requires that affected organizations:

1. Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit.
2. Identify and protect e-PHI against reasonably anticipated threats to the security or integrity of the
3. Protect e-PHI against reasonably anticipated, impermissible uses or disclosures.
4. Ensure compliance by their workforce

Considering the prevalence of accessing, sending and receiving e-PHI via email, and the vulnerabilities of doing so, it is obvious that HIPAA's call for safeguards extend to email security.

While the Safeguards Rule fails to explicitly detail the technologies and solutions organizations should implement to secure their messaging systems, it does outline a framework of **technical controls.**

These Include…

Access Controls

A covered entity must implement technical policies and procedures that allow only authorized persons to access e-PHI.

Audit Controls

A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.

Integrity Controls

A covered entity must implement policies and electronic measure to ensure that e-PHI is not improperly altered or destroyed.

Transmission Security

A covered entity must implement technical security measures that guard against unauthorized access to e-PHI, which is being transmitted over an electronic network.

How Can My Organization Meet These Requirements?

As every organization uses e-PHI and email in its own way, HIPAA does not mandate the implementation of specific HIPAA compliant email solutions to meet technical requirements. Instead, HIPAA allows affected organizations to use any security measures that allow them to appropriately implement these technical controls that ensure the integrity and security of e-PHI accessed via email.

In the maze of email security technologies, fortunately there are several that stand out as clear solutions to HIPAA requirements…

End-to-end encryption

Securing the confidential transmission of e-PHI demands an end-to-end solution to ensure that data remains confidential and secure between the message sender and the intended recipient, preventing unauthorized access or loss of e-PHI.

Data Leak Prevention (DLP)

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

Archiving

An effective email archiving system will enable your organization to meet control objectives for auditing 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.

Anti-spam and anti-virus

Protections from spam, phishing, and malware at the email gateway such as email filters and antivirus software will also demonstrate adequate protections against unanticipated threats to the integrity and security of e-PHI.

CipherPost Pro® offers healthcare providers the most flexible solution to help address HIPAA technical security safeguard standards for email and file transfer.

CipherPost Pro®

- Helps address HIPAA technical security safeguard standards for secure and confidential email transmission of e-PHI.
- 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.
- Enables Secure e-Statements for secure and traceable invoicing for medical services.
- 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.

“AppRiver gets it. They understand the security challenges health care professionals face at all levels, every day, with services designed to protect patient data, safeguard networks and keep your organization compliant with HIPAA and other privacy regulations.”

Jim Donaldson

Director of Corporate Compliance

BAPTIST HEALTH CARE

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.