HIPAA and Email Security for Healthcare Organizations

As patients demand greater protection of their information, healthcare organizations must ensure that patient privacy and their information is protected throughout any digital exchange. This white paper will describe what is required to protect that information and how to go about ensuring information security.

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. Such uses include:

- **Provider-to-Provider Communication:** Healthcare providers often need to communicate with other providers efficiently and effectively, transferring patients' medical histories, lab results, and the like to provide quality care to patients.
- **Requesting Health Consultation or Appointment:** With patients' busy schedules, and crowded waiting rooms, patients use email to request consultation and appointments before visiting a physician.
- **Submitting Health Claims to Plan Providers:** Healthcare plan providers are accepting and responding to claims submissions via email to streamline and expedite the claims process.
- **Medical Billing and Invoicing:** With email, healthcare providers can streamline and reduce the cost of paper billing.

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.

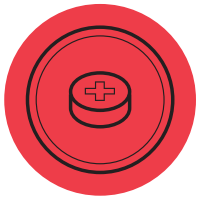
This white paper briefly details how HIPAA affects email security for healthcare organizations, and what technologies organizations can implement to help ensure secure, HIPAA-compliant email communication and file transfer.

cirius

Secure Messaging

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?

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 noncompliance. 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 does HIPAA require for email compliance?

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 email compliance.

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.

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 information.
3. Protect e-PHI against reasonably anticipated, impermissible uses or disclosures.
4. Ensure compliance by their workforce.

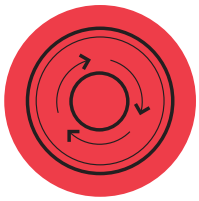
Considering the prevalence of accessing, sending and receiving e-PHI via email, and the vulnerabilities of doing so, it is obvious that HIPAA's call for safeguards extend to email security. While the Safeguards Rule fails to explicitly detail the technologies and solutions organizations should implement 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 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.



Secure email shouldn't change your workflow

As healthcare moves into the digital (IT) age, the use potential for email as a business tool is enormous: Physicians can now consult without leaving the office, healthcare providers can bill patients quickly, and patients can submit claims online, just to name a few. **When considering a solution for secure email, it's important that it conforms to HIPAA requirements without compromising the functionality and workflow of existing email.** Email security should complement existing email, not complicate it. This means implementing a solution that allows easy and scalable deployment, simplifies management complexity, and works with your existing email infrastructure to enable user-productivity and email functionality.

Cirius Secure Messaging is a cloud solution for email encryption, secure file sharing, and secure e-signatures that helps address HIPAA technical security safeguard standards while letting you use your email just the way it is.

- Helps address HIPAA technical security safeguard standards for secure and confidential email transmission of ePHI.
- Simplifies the complexity of secure electronic communications, integrating seamlessly with any email platform including MS Outlook, MS Office 365, Gmail (for both sender and recipients regardless of their network configuration).
- Enables secure file sharing of large files such as medical scans (X-rays) and other large files.
- Enables secure e-signatures in seconds right from the email window.
- Enables secure web forms for capturing information directly from your website such as doctor consultations via email, insurance claims, etc.
- 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.

Cirius Secure Messaging offers healthcare providers the most flexible solution to help address HIPAA technical security safeguard standards for email and file sharing.

About Cirius

At Cirius, we believe that email security should complement your email, not complicate it. Our cloud-based solution for secure messaging, secure e-signatures, secure large file sharing, and more works seamlessly with your email to enable secure communication and collaboration anytime, anywhere.

cirius

Secure Messaging