



# HIPAA Email Security Management in Email Communications

Secure Email White Paper

By Brenda K. Burton and Erik Kangas, PhD

## Contents

1. Overview of HIPAA
2. Provisions of the HIPAA Security Rule
3. Risk Analysis
4. Importance of Encryption for Email Communication
5. Questions to Consider When Choosing and Email Service Provider
6. A Scalable, Flexible and HIPAA-Compliant Solution in Electronic Communications
7. Chart of LuxSci Services and the HIPAA Rules they Satisfy
8. References

Performing daily business transactions through electronic technologies is an accepted, reliable and necessary tool across the nation's healthcare sectors. Therefore, electronic communications have become a standard in the healthcare industry as a way to conduct business activities that commonly include:

- Interacting with web-savvy patients;
- Real time authorizations for medical services;
- Transcribing, accessing and storing health records;
- Appointment scheduling; and
- Submitting claims to health plan payers for payment of the services provided.

Collaborative efforts amongst healthcare providers have improved the delivery of quality care to patients in addition to the recognized increase in administrative efficiency through effective use of email and other types of electronic communication. Patients are becoming more comfortable with emailing their physician's office to schedule an appointment, discuss laboratory results or request refills on medication. Medicare and some other insurance payers also recognize and pay for "online consultations" where the health provider and patient interact over the web (telemedicine).

Using the web, undoubtedly, poses concerns about the privacy and security of an individual's information. In healthcare, the confidentiality of a patient's information has been sacred since the days of the Hippocratic Oath (Hippocrates – the Father of Medicine, 400 B.C.). Today, merely taking an oath to respect one's privacy has been overshadowed by regulations that govern how certain healthcare establishments must handle an individual's health information. So, if a healthcare organization employs email as a means of communicating medical and/or mental health data to appropriate parties, they must also ensure that information is safeguarded.



This white paper will address the specific issues that a healthcare provider must address in order to be in compliance with HIPAA. It will also lay out how Lux Scientiae (LuxSci) enables providers to meet these requirements through email outsourcing.

## Overview of HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) implemented new rules for the healthcare world. Mandating compliance with its Privacy and Security Rules, the federal government is committed to enforcing patients' rights. Industry professionals – financial, administrative and clinical – are no strangers to the regulatory compliance culture. HIPAA laws apply to a 'covered entity'; i.e. healthcare providers, clearinghouses and health plan payers that meet certain conditions. In essence, most providers are covered entities if they employ an electronic-based office – meaning they function by storing and exchanging data via computers through intranets, Internet, dial up modems, DSL lines, T-1, etc.

HIPAA email security applies specifically to protected health information, not just personal information. Protected Health Information (PHI), as defined in HIPAA language, is *health information of an identifiable individual that is transmitted by electronic media; maintained in any electronic medium; or transmitted or maintained in any other form or medium*. For example, all administrative, financial, and clinical information on a patient is considered PHI.

- **Privacy Standards:** The HIPAA Privacy Rule sets standards for protecting the rights of individuals (patients). Covered entities must follow the laws that grant every individual the right to the privacy and confidentiality of their health information. Protected Health Information is subject to an individual's rights on how such information is used or disclosed.  
**Privacy Standard Key Point:** Controlling the use and disclosure of oral, written and electronic protected health information (any form).
- **Security Standards:** Taking the Privacy Rule a step further, HIPAA implemented the Security Rule to cover electronic PHI (ePHI). To this end, more secure and reliable information systems help protect health data from being "lost" or accessed by unauthorized users.  
**Security Standard Key Point:** Controlling the access to electronic forms of protected health information (not specific to oral or written).

The Privacy and Security Rules focus on information safeguards and require covered entities to implement the necessary and appropriate means to secure and protect health data. Specifically, the regulations call for *organizational and administrative requirements along with technical and physical safeguards*.

## Provisions of the HIPAA Email Security Rule

The HIPAA language uses the terms 'required' and 'addressable.' *Required* means that complying with the given standard is mandatory and, therefore, must be complied with. *Addressable* means that the given standards must be implemented by the organization unless assessments and in depth risk analyses conclude that implementation is not reasonable and appropriate specific to a given business setting. Important Note: Addressable does not mean optional.



With regard to *addressable*, an organization should read and decipher each Security standard separately and deal with each piece independently in order to determine an approach that meets the needs of the organization.

The General Rules of the Security Standards reflect a “technology-neutral” approach. This means that there are no specific technological systems to employ and no specific recommendations, just so long as the requirements for protecting the data are met.

*Organizational requirements* refer to specific functions a covered entity must perform, including the use of business associate contracts and the development, documentation and implementation of policies and procedures.

*Administrative requirements* guide personnel training and staff management in regard to PHI and require the organization to reasonably safeguard (administrative, technical and physical) information and electronic systems.

*Physical safeguards* are implemented to protect computer servers, systems and connections, including the individual workstations. This section covers security concerns related to physical access to buildings, access to workstations, data backup, storage and obsolete data destruction.

*Technical safeguards* affect PHI that is maintained or transmitted by any electronic media. This section addresses issues involving authentication of users, audit logs, checking data integrity, and ensuring data transmission security.

## Risk Analysis

Risks are inherent to any business and, therefore, with regard to HIPAA, each organization must take into consideration the potential for violating an individual’s right to privacy of their health information. HIPAA allows for scalability and flexibility so that decisions can be made according to the organization’s approach in protecting data. Covered entities must adopt certain measures to safeguard PHI from any “reasonably anticipated” hazards or threats. After a thorough risk analysis, an assessment of the organization’s current security measures should be performed. Additionally, a cost analysis will add another important component to the entire compliance picture. A plan to implement secure electronic communications starts with reviewing the Security Rule and relating its requirements to the available solution.

Below are the *administrative* and *physical safeguards* as outlined in the Federal Register. These requirements are items that must generally be addressed internally, even if you are outsourcing your email.



Standard: ADMINISTRATIVE SAFE-GUARDS	Section(s)	Implementation Specification	Required or Addressable
Security Management Process	164.308(a)(1)	Risk Analysis	R
		Risk Management	R
		Sanction Policy	R
		Information System Activity Review	R
Assigned Security Responsibility	164.308(a)(2)		R
Workforce Security	164.308(a)(3)	Authorization and/or Supervision	A
		Workforce Clearance Procedures	R
		Termination Procedures	A
Information Access Management	164.308(a)(4)	Isolating Health Care Clearing-house Function	R
		Access Authorization	A
		Access Establishment and Modification	A
Security Awareness and Training	164.310(a)(5)	Security Reminders	A
		Protection from Malicious Software	A
		Log-in Monitoring	A
		Password Management	A
Security Incident Procedures	164.308(a)(6)	Response and Reporting	R
Contingency Plan	164.308(a)(7)	Data Backup Plan	R
		Disaster Recovery Plan	R
		Emergency Mode Operation Plan	R
		Testing and Revision Procedure	A
		Applications and Data Criticality Analysis	A
Evaluation	164.308(a)(8)		R
Business Associates Contracts and Other Arrangement.	164.308(b)(1)	Written Contract or Other Arrangement	R



Standard: PHYSICAL SAFEGUARDS	Section(s)	Implementation Specification	Required or Addressable
Facility Access Controls	164.310(a)(1)	Contingency Operations	A
		Facility Security Plan	A
		Access Control and Validation Procedures	A
		Maintenance Records	A
Audit Controls	164.312(b)		R
Integrity	164.312(c)(1)	Mechanism to Authenticate EPHI	A
Workstation Use	164.310(b)		R
Workstation Security	164.310(c)		R
Device and Media Controls	164.310(d)	Disposal	R
		Media Re-use	R
		Accountability	A
		Data Backup and Storage	A

Standard: PHYSICAL SAFEGUARDS	Section(s)	Implementation Specification	Required or Addressable
Facility Access Controls	164.310(a)(1)	Contingency Operations	A
		Facility Security Plan	A
		Access Control and Validation Procedures	A
		Maintenance Records	A
Audit Controls	164.312(b)		R
Integrity	164.312(c)(1)	Mechanism to Authenticate EPHI	A
Workstation Use	164.310(b)		R
Workstation Security	164.310(c)		R
Device and Media Controls	164.310(d)	Disposal	R
		Media Re-use	R
		Accountability	A
		Data Backup and Storage	A



## Importance of Encryption for Email Communication

The security risks for email commonly include unauthorized interception of messages en route to recipient and messages being delivered to unauthorized recipients. These risks in using the Internet are addressed in the Security Rule's technical safeguards section, particularly:

- Person or Entity Authentication – *required* procedures must be implemented for identification verification of entity or party requesting access to PHI. This means the identity of the person seeking information must be confirmed within the information system being utilized.
- Transmission Security – *addressable* data integrity controls and encryption reasonable and appropriate safeguards.

Each healthcare organization using email services must determine, based on technologies used for electronic transmission of protected health information, how the Security standards are met.

*Addressable* specifications include automatic logoff, encryption, and decryption. Covered entities must also assess organizational risks, to determine if the implementation of transmission security is applicable. This includes integrity controls to ensure electronically-transmitted PHI is not improperly modified without detection. Encryption of ePHI is also addressable and not a requirement under HIPAA regulations, however, a heightened emphasis has been placed on encryption due to the [risks and vulnerabilities of the Internet](#).

Ultimately, according to the Department of Health and Human Services, a covered entity can exercise one of the following options in regard to addressable specifications:

- Implement the specified standard;
- Develop and implement an effective security measure to accomplish the purpose of the stated standard; or
- If the specification is deemed not reasonable and appropriate for the covered entity but the standard can still be met, then do not implement anything.

“Reasonable and appropriate“ relates to each organization’s technical environment and the security measures already in place.

## Important Considerations When Choosing an Email Service Provider

When your organization is responsible for critical data such as protected health information, choosing an email provider is more than a matter of trust. You should find out if the email service provider builds on the administrative, physical and technical safeguards while delivering to its customers:

- Solutions that meet or exceed HIPAA’s Security Standards
- Protection of data integrity
- Flexible, scalable services – no account is too small
- Administrative access to assign or change a user’s password
- Controls to validate a user’s access



- Audit controls to track user access and file access
- User access restrictions based on role or function
- Automatic log off after specified time of inactivity
- Data transmission security
- Unlimited document or email transfer
- Ability for encryption
- Emergency access for data recovery
- Minimal server downtime
- Secure data backup and storage
- Secure data disposal
- User friendly, web-based access without the necessity of third party software
- Privacy in not selling or sharing its client contact information

## **A Scalable, Flexible and HIPAA-Compliant Solution in Electronic Communications**

Lux Scientiae (LuxSci for short) offers secure, premium email services including extensive security features, Spam and virus filtering, robustness, and superior customer service. Our offerings are scalable to any size healthcare organization. With consistent management on LuxSci's part, your small practice or large organization will experience true email security. Take a look at the table on the following pages to see examples of how LuxSci is able to meet HIPAA's requirements for protecting electronic communications in your organization.

Healthcare staff using LuxSci can send and receive email from anywhere in the world using existing or new email clients or web browsers. Meet HIPAA's Security Standards with fierce firewalls and intrusion detection. A comprehensive solution for a complex law – managed by your account administrators in-house or remotely by our company. Risk assessments for potential HIPAA violations can be performed by administrators through the use of audit trails. Reliability and cost effective solutions are the backbone of LuxSci – even for extremely large client organizations. And, count on the physical security of our servers (the same server location the U.S. Olympic Committee employed in Salt Lake City!).



## Chart of LuxSci Services and the HIPAA Rules they Satisfy

If you are interested in specific services at LuxSci and would like to know exactly which of the HIPAA rules each service meets, the following chart will assist you. Please contact LuxSci for more information.

HIPAA Rule	1. View Email with Secure WebMail, POP, or IMAP	2. Send Email with Secure WebMail or SMTP	3. End-to-End Encryption with SecureLine combined with 1 and 2	4. Secure Collaboration (Web Aides)
Access Control - Unique User Identification	✓	✓	✓	✓
Access Control - Emergency Access	✓	✓	✓ (b)	✓ (b)
Access Control - Automatic Logoff	✓	✓	✓ (b)	✓ (b)
Audit Controls	✓ (c)	✓ (c)	✓	✓
Integrity	✓ (c)	✓ (c)	✓	✓
Person or Entity Authentication	✓	✓	✓	✓
Transmission Security > Integrity Controls	✓	✓	✓	✓
Transmission Security > Encryption	✓	✓	✓	✓
Device and Media Controls > Data Backups	✓	✓	✓	✓
Device and Media Controls > Data Disposal	✓	✓	✓	✓

(a) Our secure document storage service and use of SecureLine for communications may assume that the recipients have special passwords for their "Secure data access certificates" (PGP or S/MIME). These passwords can be stored in "Escrow," a special secure password database if the users so choose. In these cases, passwords can be retrieved in case of emergency or in case of loss.

(b) Our secure document storage service and use of SecureLine for communications encrypts data so that only the intended recipient(s) can ever view the data. The encryption process also allows the recipient(s) to verify that the data was not altered since it was sent or stored.

(c) SSL/TLS solutions encrypt the message during transport to and from LuxSci's servers and your personal computer. Email sent from LuxSci to external addresses is not necessarily secured without the use of SecureLine (Solution #3).

Solution #3 provides complete transport layer and end-to-end email security compatible with any email user anywhere, no matter what software s/he may have.

## References

Health Insurance Reform: Security Standards – Federal Register, Vol. 68, No. 34, 45 CFR Parts 160, 162, 164.  
[Centers for Medicare and Medicaid HIPAA Security Series](#)