

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.

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 implicit since 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.

Below, you can see how PrivacyHarbor enables you to meet these requirements though the use of our application.

PrivacyHarbor.com offers secure, private email services including extensive security features, Spam and virus filtering, robustness, and superior customer service. Their offerings are scalable to any size healthcare organization. With consistent management on PrivacyHarbor.com’s part, your small practice or large organization will be able to send and receive messages securely. Take a look at the table below to see examples of how PrivacyHarbor.com is able to meet HIPAA’s requirements for protecting electronic communications in your organization.

Standard: TECHNICAL SAFEGUARDS	Sections	Implementation Specification	Required or Addressable
Access Control	164.312(a)(1)	Unique User Identification	R
HIPAA COMPLIANT SOLUTION from PrivacyHarbor.com			
The Rule States: “Assign a unique name and/or number for identifying and tracking user identity.”			
Solution: Use of unique usernames and passwords for all user accounts.			
Standard: TECHNICAL SAFEGUARDS	Sections	Implementation Specification	R/A
		Emergency Access Procedure	R

HIPAA COMPLIANT SOLUTION from PrivacyHarbor.com			
<p>The Rule States: <i>“Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency”</i></p> <p>Solution: PHI in email communications can be accessed from any location via the Internet. There are also mechanisms for authorized administrative access to account data.</p>			
Standard: TECHNICAL SAFEGUARDS	Sections	Implementation Specification	R/A
		Automatic Logoff	A
HIPAA COMPLIANT SOLUTION from PrivacyHarbor.com			
<p>The Rule States: <i>“Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.”</i></p> <p>Solution: An organization/ individuals can set screen savers on their desktops to log users out. Additionally, our system automatically logs off all users after a predetermined amount of time;</p>			
Standard: TECHNICAL SAFEGUARDS	Sections	Implementation Specification	R/A
		Encryption and Decryption	A
HIPAA COMPLIANT SOLUTION from PrivacyHarbor.com			
<p>The Rule States: <i>Implement a mechanism to encrypt and decrypt electronic protected health information.</i></p> <p>Solution: All usernames, passwords, and all other authentication data can be encrypted during transmission to and from PrivacyHarbor servers and our clients. Additionally, our SSL Line permits end-to-end encrypted email communications with anyone on the Internet.</p>			
Standard: TECHNICAL SAFEGUARDS	Sections	Implementation Specification	R/A
Audit Controls	164.312(b)		R
HIPAA COMPLIANT SOLUTION from PrivacyHarbor.com			
<p>The Rule States: <i>“Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.”</i></p> <p>Solution: Detailed audit trails of logins are available to account administrators. These include the dates, times, and the IP addresses from which the logins were made. Auditing of all sent and received email messages is also available to administrators. also system permits auditing of when messages have been read.</p>			
Standard: TECHNICAL SAFEGUARDS	Sections	Implementation Specification	R/A
Integrity	164.312(c)(1)	Mechanism to Authenticate EPHI	A
HIPAA COMPLIANT SOLUTION from PrivacyHarbor.com			

The Rule States: *“Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.”*

“Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.”

Solution: To prevent unauthorized alteration or destruction of PHI, the use of SSL and Encryption will verify message integrity upon receipt. PLEASE NOTE PRIVACY HARBOR.COM CANNOT CONTROL PHI ONCE THEY HAVE REACHED THE INTENDED RECIPIENT. EACH ORGANIZATION/INDIVIDUAL MUST MAKE SURE THAT THEIR INTERNAL POLICIES ARE IN PLACE AS IT REGARDS ALTERATION OR DESTRUCTION ONCE RECEIVED.

Standard: TECHNICAL SAFEGUARDS	Sections	Implementation Specification	R/A
Person or Entity Authentication	164.312(d)		R

HIPAA COMPLIANT SOLUTION from PrivacyHarbor.com

The Rule States: *“Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.”*

Solution: Username and Password are used for access control; strict control is given over who can access user’s accounts. PrivacyHarbor’s privacy policy strictly forbids any access of email data without explicit permission of the user (unless there are extenuating circumstances). Also, use of end-to-end encryption and SSL in email and storage ensures that only the intended recipient(s) of messages or stored emails can ever access them.

Standard: TECHNICAL SAFEGUARDS	Sections	Implementation Specification	R/A
Transmission Security	164.312(e)(1)	Integrity Controls	A

HIPAA COMPLIANT SOLUTION from PrivacyHarbor.com

The Rule States: *“Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.”*

“Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of”

Solution: SSL-based encryption during the transmission of data to/from our clients for email and email storage services is provided. SSL-based encryption for all inbound email at PrivacyHarbor ensures that all email sent internally between PrivacyHarbor.com users meets “Transmission Security” guidelines and also provides for true end-to-end encryption of messages to/from non-clients.

Standard: TECHNICAL SAFEGUARDS	Sections	Implementation Specification	R/A
		Encryption	A

HIPAA COMPLIANT SOLUTION from PrivacyHarbor.com

The Rule States: *“Implement a mechanism to encrypt electronic protected health*

information whenever deemed appropriate.”

Solution: SSL encryption for our email service is provided. Additional services, such as message retract, messaging status and storage are also available.

Standard: TECHNICAL SAFEGUARDS	Sections	Implementation Specification	R/A
Device and Media Controls	164.310(d)	Data Backup and Storage	R

HIPAA COMPLIANT SOLUTION from PrivacyHarbor.com

The Rule States: *“Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.”*

Solution: Live data is stored on a live data base, weekly automated backups ensure exact copies of all PHI are available.

Standard: TECHNICAL SAFEGUARDS	Sections	Implementation Specification	R/A
		Data Disposal	R

HIPAA COMPLIANT SOLUTION from PrivacyHarbor.com

The Rule States: *“Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.”*

Solution: Clients can delete their data whenever desired.

Healthcare staff and their customer using PrivacyHarbor.com can send and receive email from anywhere in the world where they can access the internet and know that their communication is 100% safe, secure and private. We meet HIPAA’s Security Standards with fierce firewalls and intrusion detection. We can provide a comprehensive solution for a complex law - managed by account administrators in-house or remotely by our company. Cost effective solutions to a safe, secure and private communication system are the core values of PrivacyHarbor.com- no matter how small or large the organization. And, count on the security of our servers with the multi layer security system we have in place.

Chart of PrivacyHarbor.com Services and the HIPAA Rules they Satisfy

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

HIPAA Rule	1. View Email with our security rich service	2. Send Email with SSL – encryption technology	3. End-to-End Encryption
Access Control - Unique User Identification	✓	✓	✓
Access Control - Emergency Access	✓	✓	✓
Access Control - Automatic Logoff	✓	✓	✓
Audit Controls	✓	✓	✓
Integrity	✓	✓	✓
Person or Entity Authentication	✓	✓	✓
Transmission Security > Integrity Controls	✓	✓	✓
Transmission Security > Encryption	✓	✓	✓
Device and Media Controls > Data Backups	✓	✓	✓
Device and Media Controls > Data Disposal	✓	✓	✓

[SSL solutions](#) encrypt the message during transport to and from PrivacyHarbor.com servers and your personal computer. Email sent from PrivacyHarbor.com to out of network email addresses are not necessarily secured unless secure messaging (encryption) is maintained with the use of our encryption technology.