HIPAA HITECH 2010: Email Hosting at LuxSci

How does HIPAA HITECH 2010 affect the Business Associates of HIPAA Covered Entities?

With the new changes, HIPAA Business Associates are now responsible for following all HIPAA Privacy and Security regulations with respect to all protected health information that they obtain or generate. Business Associates themselves are also now exposed to liability and monetary and publicity penalties in the event of a HIPAA privacy breach in their systems.

How have the HIPAA HITECH 2010 changes impacted LuxSci?

In order to consider ourselves a Business Associate of a HIPAA Covered Entity under the new law, LuxSci has implemented protocols and policies to assure compliance with the new HIPAA changes for storing and transmitting Electronic Protected Health Information. These cover everything from our hardware and software infrastructure, to staff access, to internal processes, to training requirements, to our Privacy Policy.

What is Protected Health Information (PHI)?

In HIPAA language, Protected Health Information is defined as "*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. Electronic PHI (ePHI) is when this data is stored or transmitted via electronic means including email and web sites

How does HIPAA apply to email?

HIPAA expanded upon the Privacy rule by implementing the Security Rule to cover ePHI. 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, included that transmitted by email. The HIPAA Technical Safeguards cover the particular means by which to secure ePHI, with the most important requirement that email messages be encrypted and protected during the entire time they are transmitted across the Internet.

What are the specific HIPAA technical safeguards?

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. HIPAA compliant hosting accounts at LuxSci impose a range of technical security features to maximize the level of data protection and minimize the chance of a breach or other violation of HIPAA.

What is required in order to be a HIPAA-compliant account at LuxSci?

To have a HIPAA compliant account and be a Business Associate of LuxSci, you must sign and return our HIPAA Business Associate Agreement (HBAA) and our Account Restrictions Agreement (ARA). In addition, the security restrictions put in place on your account will be locked down by LuxSci support to prevent you from changing them.

What are the actual security restrictions LuxSci enforces on HIPAA-compliant accounts?

These settings are described in detail in our HIPAA Account Restrictions Agreement, however, in summary they include: minimum password length and complexity; SSL connections to all services; encryption of all outbound messages; WebMail timeout limit; secure WebAide feeds; secure use of SecureForm; no insecure off-site email forwards.

How does LuxSci meet the HIPAA technical safeguards to protect health information?

Technical safeguards affect PHI that is maintained or transmitted by any electronic media. The chart on the following pages presents our solutions to the technical safeguards as stated in the HIPAA rules. LuxSci requires that these security restrictions be enforced and locked-down on any account which is using or sending ePHI.

Technical Safeguard	Implementation Specification	R/A?*	The Rule States	LuxSci's Solution
Access Control	*Unique User Identification* Section 164.312(a)(2)(i)	R	"Assign a unique username and/or number for identifying and tracking user identity."	**Use of unique usernames and passwords for all distinct users. Requirement of minimum password strength of 8 characters, alphanumeric, plus must pass a 'crack' algorithm.**
	Emergency Access Procedure Section 164.312(a)(2)(ii)	R	"Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency."	**PHI in email communications can be accessed from any location via the Internet. There are also mechanisms for authorized administrative access to account data.**
	Automatic Logoff Section 164.312(a)(2)(iii)	A	"Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity"	**WebMail auto-logoff for all users after 20 minutes of inactivity. Other services, such as POP, IMAP, and SMTP also have automatic logoffs.**
	Encryption and Decryption Section 164.312(a)(2)(iv)	A	"Implement a mechanism to encrypt and decrypt electronic protected health information"	**All communications between the user and LuxSci's servers are over secure SSL- or TLS-encrypted connections. All outbound email must be encrypted, using any combination of TLS, S/MIME, PGP, or SecureLine Escrow web-based message pickup.**
Audit Controls	*Audit Controls* Section 164.312(b)	R	"Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or user electronic protected health information."	**Detailed downloadable audit trails of all logins to WebMail, POP, IMAP, and SMTP services are available to users and administrators. The reports include the dates, times, and the IP addresses from which the logins were made, and if they were secure or not. Auditing of all sent and received email messages is also available. Audit information for other services, such as FTP, login failures, etc., is also available if needed through Support.**

* 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 analysis conclude that implementation is not reasonable and appropriate specific to a given business setting. Important Note: Addressable does not mean optional.

Technical Safeguard	Implementation Specification	R/A?*	The Rule States	LuxSci's Solution
Integrity	*Mechanism to Authenticate ePHI* Section 164.312(c)(1)	A	"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."	**To prevent unauthorized alteration or destruction of PHI, the use of LuxSci's SecureLine and enforced connection encryption (SSL & TLS) ensures that the messages cannot be modified while in transit. Their integrity can be assured. Additionally, LuxSci's SecureLine permits the addition of digital signatures to encrypted messages to further ensure and prove the message integrity and identity of the sender.**
Person or Entity Authentication	*Person or Entity Authentication* Section 164.312(d)	R	"Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."	**Username and strong passwords are used for access control; strict control is given over who can access user's accounts. LuxSci's privacy policy strictly forbids any access of email data without explicit permission of the user (unless there are extenuating circumstances). SecureLine end-to-end encryption in email and document storage includes features that can ensure that only the intended recipient(s) can ever access them.**
Transmission Security	*Integrity Controls* Section 164.312(e)(2)(i)	A	"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."	**SSL/TLS encryption is enforced during the transmission of all data to and from our clients for all services, including WebMail, POP, IMAP, SMTP, FTP, and remote MySQL access. TLS-based encryption of inbound email at LuxSci ensures that all email sent internally at LuxSci meets "Transmission Security" guidelines and allows you to securely send and receive with other companies whose servers also support TLS. LuxSci also provides SecureLine for true end-to-end encryption of messages to/from non-clients.**
	Encryption Section 164.312(e)(2)(ii)	A	"Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate."	**SSL encryption for WebMail, POP, IMAP, SMTP, FTP, and remote MySQL services is required and forced. Additional services, such as SecureLine for encrypting email while at rest and WebAides for encrypting documents and other data while at rest are also available.**

Technical Safeguard	Implementation Specification	R/A?*	The Rule States	LuxSci's Solution
Device and Media Controls	*Data Backup and Storage* Section 164.310(d)ɟςɋɟÉÖɋ	R	"Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment."	**Daily on-site and weekly off-site backups ensure exact copies of all PHI are available. Live data is stored on redundant RAID-5 disk arrays for added protection. Furthermore, a recommended but optional service, Premium Email Archival, provides permanent, immutable storage on servers in multiple geographic locations.**
	Data Disposal Section 164.310(d)ɟςɋɟÉɋ	R	"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."	**Clients can delete their data whenever desired. Additional security comes in automatic expiration of data backups which cease to exist after 4 weeks. Alternate expiration plans are available for large clients. All media used in conjunction with ePHI is disposed of in compliance with HIPAA requirements.**