

Medical Privacy

Version 2011.04.22

Account Restrictions Agreement [ARA] - Required by LuxSci HIPAA Accounts

In order for LuxSci to ensure the security and privacy of all **Electronic Protected Health Information (ePHI)** that is stored on or that passes through its servers, [See the definition of what LuxSci considers ePHI in the [Business Associate Agreement](#)] LuxSci has instituted the following restrictions that are required of all accounts designated as HIPAA.

NOTE: A customer of LuxSci that stores ePHI on LuxSci servers and/or sends ePHI through LuxSci and who is a HIPAA Covered Entity or a Business Associate of a HIPAA Covered Entity, must be **designated and approved as a HIPAA Account** at LuxSci or be subject to account(s) suspension. By law, *it is incumbent upon LuxSci to ensure that all customers that it knows to store and/or send ePHI have a co-signed LuxSci Business Associate Agreement and be configured in a way that safeguards ePHI.*

There are two different types of HIPAA Accounts at LuxSci; the LuxSci HIPAA requirements for each type are slightly different. The two types are:

- Account-Wide HIPAA: All users and all domains in the account are locked down for compliance.
- Per-Domain HIPAA: All users have a general level of good security enforced, but only users in designated "HIPAA Domains" can use the services for ePHI and only these users are locked down for compliance.

1. Account Type Requirements

In order to be considered a HIPAA Account, a LuxSci customer account must:

- [Account-Wide HIPAA Accounts] Have SecureLine licenses for all users in Email Hosting or SecureForm accounts domains
- [Per-Domain HIPAA Accounts] Have SecureLine licenses for all users in designated HIPAA
- Use a Premium High Volume Outbound Email Account for bulk email
- Be a Covered Entity under HIPAA (or a Business Associate of Covered Entity)

2. Account Security Requirements

The following security measures must be enforced on HIPAA Accounts before LuxSci will consider the customer to be taking appropriate measures to safeguard ePHI and thus be eligible for status as a HIPAA Account.

2.1 Enforced use of Secure Logins: All logins to LuxSci servers by any user in the account, must be secured via SSL, TLS, or SSH. This includes: WebMail, POP, IMAP, SMTP, FTP, and remote MySQL access.

2.2 Password Strength: All passwords used by all users to access LuxSci servers must be "strong". This means that they must be 8 or more characters long, contain both letters and numbers, and pass the "crack" password strength checking system to ensure that they are hard to guess.

2.3 Web Interface Session Timeout: The maximum web interface (i.e. WebMail) session timeout must be reduced to 20 minutes.

2.4 [Section removed as it referred to a feature no longer available].

2.5 Outbound Email Encryption Enforcement. (Enforced SecureLine Encryption will use TLS-only transport encryption for recipients whose email servers support TLS, PGP or S/MIME when available, and SecureLine Escrow for anyone else with an email address. This restriction applies to messages sent via WebMail and via SMTP. Messages sent via SMTP that cannot be encrypted or sent via TLS are blocked.)

2.5.1: [Account-Wide HIPAA] All users will be forced to have their outbound email encrypted.

2.5.2: [Per-Domain HIPAA] All users in designated HIPAA domains will be forced to have their outbound email encrypted.

2.6 WebAides Feeds: All published WebAides feeds must be accessed over a password-protected secure connection (HTTPS).

2.7 SecureForm: All SecureForms configured must be configured securely. This means that HTTPS must be used to secure the form data when it is posted and PGP, S/MIME, or TLS SecureLine encryption must be used to encrypt any email messages containing form data sent out from the SecureForm service.

2.8 Secure Forwarding Enforced: This ensures that all messages that might contain ePHI which are forwarded will be encrypted during transport using TLS. Attempts to configure forwarding to recipients using email services that do not support SMTP TLS message delivery will be uniformly restricted by the LuxSci system. The Customer can optionally further restrict end users from being able to enable any filtering and forwarding settings for themselves.

2.8.1: [Account-Wide HIPAA] All email forwarding rules for any address created using features of your LuxSci account (i.e. email aliases, email forwards, email capturing, etc.) can only be forwarded to recipients whose email servers support TLS for SMTP transport encryption.

2.8.2: [Per-Domain HIPAA] All email forwarding rules for addresses in designated HIPAA domains created using features of your LuxSci account (i.e. email aliases, email forwards, email capturing, etc.) can only be forwarded to recipients whose email servers support TLS for SMTP transport encryption.

2.9 Maximal Security Lockdown: The above configuration settings are put in place by LuxSci's "Maximal Security" tool. LuxSci Support will lock down this setting so that Account Administrators cannot change any of

the above settings themselves. Additionally, LuxSci Support cannot change any of the settings without first removing the lockdown. All changes to the settings and the lockdown itself are permanently logged in your account's audit trail.

3. Workarounds

Due to the nature of the HIPAA and HITECH requirements, as your Business Associate, LuxSci has a great deal of responsibility in ensuring that your use of its services is such that ePHI is safeguarded. As a result, LuxSci imposes the restrictions of Section 2. There are various ways to increase the usability of the system in the face of these necessary security requirements. Identified below are our recommendations. Customer is not required to be compliant with or implement any or all of the recommendations presented below; they are all optional. Failure by Customer to comply with or implement any of the recommendations identified in this Section 3 does not void or negate any obligation or responsibility of LuxSci or a Customer under this or the Business Associate Agreement.

3.1 TLS-Only Secure Delivery: SecureLine Outbound Encryption permits enabling TLS-Only delivery as an option for outbound email encryption. Recipient domains hosted by LuxSci or whose email servers support SMTP over TLS, can be delivered to "normally" without the required use of more complex outbound encryption (i.e. PGP, S/MIME, or Escrow). I.e. all messages to such recipients would be sent via "regular email"; however, that regular email would be delivered over a secure channel -- either locally within LuxSci or to remote servers over a TLS-secured channel. This kind of delivery meets HIPAA's Security Rule requirements, while allowing a large class of email messages (such as those between users in your account) to be sent and received normally.

TLS-Only secure delivery can be enabled for only selected recipient domains or can be dynamic -- where the system will dynamically determine eligible recipients and use TLS whenever possible.

3.2 Automatic Inbound Email Decryption: This optional feature will allow all inbound email encrypted via PGP or S/MIME for your users to be automatically decrypted upon arrival to LuxSci. As all email between users in your account and messages sent to them from SecureLine Escrow or SecureSend will be encrypted in this way, it allows:

- Users to access these email messages "as normal" via WebMail or their favorite email client (both over an SSL-secured channel to LuxSci's servers).
- Access to all of these received messages without any need for further manual decryption or passwords.
- Filtering of decrypted email upon arrival to LuxSci's servers using custom filtering rules that you are able to set up.
- Archival of inbound messages in an unencrypted format so that they are more easily searchable and so that they can be accessed even if the original certificates used are deleted or the passwords forgotten.
- Business as almost-usual for inbound email.

3.3 Global SecureLine Address Book: Have an account administrator create an "Address Book" in the web interface where you define all of the common contacts to whom your organization corresponds. In this Address Book, you can also upload PGP and S/MIME public keys, should they be available, or specify a question and answer that should be used when picking up secure emails via SecureLine Escrow. This Address Book can be

shared with all users in your account (and they can be auto-subscribed to it), so that it is automatically used when your users are sending email messages (via WebMail and SMTP). Not only do your users get easy access to the shared contact list, but the security information being used can be centrally located and managed.

3.4 Default SecureLine Escrow Question and Answer: For outbound email messages going to recipients who do not support TLS and have not been explicitly set up in the system or in a shared Address Book, you can define a default question and answer that will be used to secure a SecureLine Escrow message to them. This allows you to send to any email address without needing to pre-configure it. This is especially useful when using SMTP as, unlike WebMail, you cannot specify a new SecureLine Escrow question and answer in your email client at the time of sending.

3.5 Control Email Forwarding: Even though email forwarding is restricted to be to TLS-enabled recipients only, you still have responsibilities with regard to forwarding. Administrators can choose to restrict end users from managing their own email forwarding and filtering settings. By requiring only Account Administrators to configure these settings, you can easily ensure that only approved email forwarding rules are in place. Additionally, instead of forwarding email messages to external accounts, custom email filters can be used to send non-ePHI-containing notices of messages arrivals to any external email address. In this way, users can be informed of the arrival of messages in their insecure accounts, without potential ePHI being forwarded out of their secure accounts.

3.6 Multiple Sending Profiles: For users who must be able to send some messages securely and some insecurely (to non-exempt domains), LuxSci recommends having two separate domains -- one regular and one HIPAA. For example "john@yourdoctor.com" for regular email and "john@secure.yourdoctor.com" for ePHI. The recommendation for separate user logins is based on the following:

- These two accounts can be setup in parallel in the user's email program (i.e. Outlook or Thunderbird).
- The user can select the appropriate email account by choosing the account in the email program before sending. I.e. Click on the "Secure" account to send ePHI and the "insecure" account to send non-ePHI.
- The user can see inbound email arriving to either account in real time in his/her email program.
- The user can reply to messages as normal in his/her email program.
- The user can reply to an "insecure" message securely by dragging and dropping it from the insecure inbox to the secure inbox before sending (among other ways).
- The separate domains with LuxSci keep the delineation of what is ePHI and what is not ePHI, very clear.
- The separate accounts in the user's email client keep the distinction of what is secure and not, very clear.
- *It is up to your end user to determine what should be sent securely or not.*
- The recipient also gains assurance via the different email address "secure.yourdoctor.com" that s/he sees when receiving a message containing ePHI.
- Your "insecure" login with LuxSci will not be forced to send email in an encrypted manner.

This approach is really the cleanest way to separate secure from insecure email in terms of clarity and ease of use for the end user and in terms of limiting liability for improper disclosure of ePHI for both you and LuxSci.

4. Customer Responsibility

LuxSci cannot reasonably lockdown all aspects of an account to prevent any possible use that might disclose ePHI in an unauthorized fashion. As a result, with respect to the terms specified in the LuxSci HIPAA Business Associate Agreement, it is the *HIPAA Customer's responsibility* to ensure that all ePHI in the following situations is safeguarded appropriately.

4.1 Email Forwarding: LuxSci gives Customers the ability to automatically forward email messages from their LuxSci email account to external email addresses that support TLS for secure email transmission. In this way, any potential ePHI is forwarded out of the account in a secure, encrypted manner. This feature is mainly intended to make it easy to integrate LuxSci services with those of other secure email servers. *It is the Customer's responsibility to ensure that email is not forwarded to locations that could result in violations of the HIPAA Security or Privacy Rules. Customer is responsible for preventing any HIPAA breach due to improper use or disclosure of ePHI resulting from ePHI being forwarded to improper recipients or insecure locations.* For example, **forwarding email to other Customer-controlled accounts at LuxSci or other service providers which are NOT HIPAA-compliant would render Customer not HIPAA-Compliant in general and would be a violation of this Agreement.**

4.2 Email Sending: LuxSci gives Customers the ability to send email to anyone on the Internet and have that email be transmitted to the recipient(s) in a secure and encrypted manner. It is the Customer's responsibility to ensure that ePHI is only transmitted to recipients whose access to that ePHI would not violate the HIPAA Privacy Rule. *Customer is responsible for preventing any HIPAA breach due to improper use or disclosure of ePHI resulting from ePHI being emailed to improper recipients.*

4.3 Web Sites: HIPAA Customers are in full control of the content and operation of any hosted web sites. LuxSci does not perform audits of these sites to ensure that they are constantly HIPAA compliant. *HIPAA Customer must ensure that any ePHI stored on or accessible through or submitted to its web site(s) is safeguarded to a degree that satisfies the HIPAA Security and Privacy rules.* This may include:

- Use of SSL and password protection to secure portions of the web site.
- Storing data in an encrypted fashion.
- Using LuxSci's SecureForm service for processing form submissions that may contain ePHI.
- Removing any unencrypted ePHI from the customers' web or file storage areas.

4.4 File Storage: HIPAA Customers using shared web hosting servers (as opposed to dedicated servers) must not have any unencrypted ePHI stored in any files in the shared web / FTP file storage space. Additionally, any files containing passwords to databases or encryption keys must be secured by permissions to ensure that other users on the same shared server cannot gain read or write access.

4.5 McAfee Outbound Filtering: Customers using outbound email services from McAfee must be sure that they are using TLS to encrypt the messages sent from their workstations or servers to McAfee. Alternately, they should relay such messages securely through LuxSci's outbound email servers -- LuxSci's servers can then ensure secure relaying of the messages through McAfee.



4.6 McAfee Email Archival: Customers using Premium Email Archival (provided through our partnership with McAfee) must configure a secure connection for the ingest of the messages into the archival system. LuxSci automatically configures the archival account in this way for customers whose email is hosted with LuxSci, and this is enforced by policy. For customers who are ingesting email from their own servers, it is their responsibility to be sure that this connection is secure.

4.7 Premium Email Filtering: Customer has access to the Premium Email Filtering control panel at McAfee. Customer must ensure that:

- Any email forwarding to distribution lists or notification email addresses configured in this portal are only delivered to recipients in their filtered domains -- forwarding to other email addresses may result in the messages being delivered without transport encryption to the recipient(s).

4.8 LDAP: Customers using LDAP for access to their Address Books must use LDAP over SSL if their address books may contain ePHI.

4.9 Widgets: Customers must not implement custom or third party Widgets in the LuxSci user interface which might be used for transferring/storing ePHI at third party locations in a manner which does not safeguard that data. LuxSci does not include the data in or passing through third party Widgets to be in its definition of supported ePHI.

4.10 Other Email Accounts: It is the Customer's responsibility to inform LuxSci of all accounts that they may have with LuxSci which may be involved in the sending, receipt, or storage of ePHI.

4.11 Access Auditing: It is the Customer's responsibility to review the access auditing reports for individual users if that is deemed by Customer to be important for their HIPAA compliance. Only Customer would have clear knowledge as to what access is legitimate and what is not.

4.12 Sharing: Customers in Per-Domain HIPAA accounts are permitted to share objects (such as email folders, workspaces, and WebAides) owned by non-HIPAA users with HIPAA users. It is the Customer's responsibility to either (a) restrict sharing by end users so that this is not permitted, or (b) to ensure that HIPAA users never copy ePHI into the shared objects of non-HIPAA users thus permitting access to ePHI by non-compliant users.



5. Agreement

Please sign and date this document to indicate that you agree with the required restrictions that will be imposed on a HIPAA account (Section 2) and that you understand your own responsibility in safeguarding ePHI with respect to your LuxSci account (Section 4).

Customer Name & Title

Signature & Date

Account or Order #: _____

All pages are required to be returned to LuxSci.

Fax: 413-332-0598

Email: sales@luxsci.us

Postal Address: Lux Scientiae, Inc.
Box 326
Westwood, MA 02090