Account Restrictions Agreement [ARA]

Required by LuxSci HIPAA Accounts

Version 2018.03.26

In order for Lux Scientiae, Incorporated (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 protects as potential ePHI in the Business Associate Agreement]. LuxSci has instituted the following restrictions that are required of all HIPAA Customer accounts.

NOTE: A customer of LuxSci that stores ePHI on LuxSci servers and/or transmits 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-customer 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 who store and/or transmit ePHI in or through LuxSci services have a cosigned Business Associate Agreement with LuxSci and be configured in a way that safeguards ePHI.*

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

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

1. Account Type Requirements

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

- [*Account-wide HIPAA Accounts*] Have SecureLine licenses for all users
- [*Per-domain HIPAA Accounts*] Have SecureLine licenses for all users in designated HIPAA-compliant domains plus the main administrator of the account.
- Use a Premium High Volume outbound email account for bulk email or transactional email
- Be a Covered Entity or Business Associate under HIPAA
- Have signed a Business Associate Agreement and (this) Account Restrictions Agreement with LuxSci.
- Have their account configured and locked down with the minimum account security requirements denoted in Section 2.

2. Account Security Requirements

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

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

www.luxsci.com
sales@luxsci.com
1.800.441.6612
LuxScientiae, Inc.
P.O. Box 326
Westwood, MA 02090

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 a minimum password entropy 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 4 hours or less. A timeout of 20 minutes is recommended.

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

2.5 Outbound Email Encryption Enforcement. Use of LuxSci SecureLine for outbound email encryption must be enabled for email being sent from LuxSci. Customer may choose to allow individual users to opt out of encryption on a per-message basis by certifying that a message contains no ePHI. (SecureLine Encryption may use any of: TLS-only-transport encryption, PGP, S/MIME, or SecureLine Escrow for email encryption.)

2.5.1 [Account-wide HIPAA] All email hosting users (i.e., those that can send and/or receive email via LuxSci) in the account must have SecureLine outbound email encryption enabled.

2.5.2 [Per-domain HIPAA] All email hosting users in designated HIPAA-compliant domains must have SecureLine outbound email encryption enabled.

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

2.7 SecureForm: All SecureForms must be configured “securely.” This means that form submissions must be transported over HTTPS, that and PGP, S/MIME, SecureLine Escrow, or Forced TLS encryption methods must be used to encrypt any email messages containing form data sent out from the SecureForm service, that secure FTP must be used for any FTP uploads, and that other appropriate measures must be taken, as appropriate, to protect potential ePHI as it is stored in or transported through LuxSci's SecureForm service.

2.8 Secure Email Forwarding Enforced: This ensures that all messages that might contain ePHI which are forwarded will be encrypted during transport to the recipients using TLS. Attempts to configure forwarding to recipients that use email services that do not support SMTP TLS message delivery will be uniformly restricted by the LuxSci system. HIPAA 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 (e.g. 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-compliant 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. **WebAides**: Auditing of Blog, Document, and Password WebAides will be enabled and enforced. Additionally, optional entry-level encryption for Blog and Document WebAides can be enabled.

www.luxsci.com
sales@luxsci.com
1.800.441.6612
LuxScientiae, Inc.
P.O. Box 326
Westwood, MA 02090

2.10 Maximal Security Lockdown: The above configuration settings are put in place by LuxSci's "Maximal Security" tool. LuxSci Support will lock down Customer accounts 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.

2.11 Dedicated Web Hosting: In addition to securing the dedicated web hosting server environment, applying timely patches, configuring and updating firewalls, performing automated virus scans, performing automated server vulnerability scans, providing access controls and keeping audit logs, watching for intrusions and other activities, LuxSci locks down dedicated web servers with the following security controls:

2.11.1 Dedicated servers are required for HIPAA-compliant web sites
2.11.2 “root” server access is never provided to customers
2.11.3 “sudo” access is generally restricted; sudo access to very specific commands is only granted after a security review of the impact of said access and then only if there is a very strong need for said access
2.11.4 Direct access to “php.ini” and global Apache configuration files is restricted. Changes to such configurations must be approved by and made by LuxSci support.
2.11.5 Direct configuration of “crontab” is restricted. Changes to such crontab must be approved by and made by LuxSci support.
2.11.6 Only secure channels for server management are permitted (i.e. HTTPS, SFTP, and SSH).

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 implement any of the recommendations presented below; they are all optional. Failure by Customer to implement any of the recommendations identified in this Section 3 does not void or negate any obligation or responsibility of LuxSci or Customer under this or the Business Associate Agreement.

3.1 TLS-only Secure Delivery: (Enabled by default) SecureLine 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 mechanisms (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 using SMTP TLS. This kind of delivery meets HIPAA's Security Rule minimal requirements, while allowing a large class of email messages (such as those between users in your account) to be sent, received, and accessed in away that appears "normal."

TLS-only secure delivery can be enabled for only selected recipients and/or domains, or can be dynamic ------ where the system dynamically determines eligible recipients and uses SMTP TLS whenever possible.

www.luxsci.com
sales@luxsci.com
1.800.441.6612
LuxScientiae, Inc.
P.O. Box 326
Westwood, MA 02090

3.2 Automatic Inbound Email Decryption: This optional feature will allow all inbound email to your users which is encrypted via PGP or S/MIME to be automatically decrypted upon arrival to LuxSci. When using PGP or S/MIME for transport encryption, this enables:

- Users to access these email messages "as normal" via WebMail or their favorite email client (both over a TLS-secured channel to LuxSci's servers).
- Access to all of these received messages without any need for further manual decryption.
- Filtering of decrypted email upon arrival to LuxSci's servers using custom filtering rules.
- 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 PGP- and S/MIME-encrypted inbound email.

3.3 Global SecureLine Address Book: Have an account administrator create an "Address Book" in the Web interface where common contacts to whom your organization corresponds can be defined. In this address book, you can upload PGP and S/MIME public keys, should they be available, or specify a question and answer pairs that should be used to verify recipient identity when picking up secure emails via SecureLine Escrow. This address book can be shared with some or all users in your account so that it is automatically used when these users send email messages (via WebMail or SMTP). Not only do these 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 that are using SecureLine Escrow for encryption, you can define a default question and answer that will be used to authenticate access to their messages. This default question and answer is used in cases where a more specific question and answer has not been defined in address books and other recipient-specific authentication information is not available. Use of a default question and answer allows you to send to any email address without needing to pre-configure it or to require recipients to create SecureSend accounts.

3.5 SecureSend Recipient Authentication for Escrow: (enabled by default) For outbound email messages going to recipients via SecureLine Escrow, you can configure SecureLine so that the recipients are required to register for a free "SecureSend" account and then use that password to authenticate their access to all SecureLine Escrow messages received. This precludes the need to define "questions and answers" for your recipients and to communicate those to them.

3.6 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 message arrivals to any external email address. In this way, users can be informed in their insecure accounts of the arrival of messages to their secure accounts, without potential ePHI being forwarded out of their secure accounts.

3.7 Opting Out of Outbound Email Encryption: HIPAA Customers can choose to allow users to opt out of outbound email encryption on a per-message basis by requiring the sender to certify which messages does not contain any ePHI. This is not enabled by default; enabling it places the responsibility for the proper classification of messages as ePHI-containing or not on the HIPAA Customer.

www.luxsci.com
sales@luxsci.com
1.800.441.6612
LuxScientiae, Inc.
P.O. Box 326
Westwood, MA 02090

3.8 Multiple Sending Profiles: For users who must be able to send some messages securely and some insecurely, LuxSci recommends having two separate domains ------ one regular and one HIPAA compliant. 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 (e.g. Outlook or Thunderbird).
- The user can select the appropriate email account by choosing the account in the email program before sending. E.g. 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 and what does not contain ePHI.*
- The recipient also gains assurance via the different email address "secure.yourdoctor.com" that s/he sees when receiving a message containing ePHI.
- The non-HIPAA-compliant logins 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.

3.9 Mutual Consent. HIPAA permits the sending of ePHI insecurely to patients under Mutual Consent (where the patients have requested insecure delivery, secure options are available, and where the patients have been educated on the risks). Messages containing ePHI that are sent insecurely are permitted under Mutual Consent. Doing so may require sending from a non-HIPAA user account or may require using the "HIPAA Opt-Out" feature.

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 configure rules that 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 HIPAA-compliant 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 could render Customer not HIPAA-compliant in general and would be a violation of this Agreement.**

www.luxsci.com
sales@luxsci.com
1.800.441.6612
LuxScientiae, Inc.
P.O. Box 326
Westwood, MA 02090

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 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 TLS and password protection to secure portions of the web site.
- Storing data encrypted at rest.
- 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.
- Maintaining proper access controls, audit trails, and data backups.
- Performing periodic code reviews, penetration tests, risk assessments, and remediation
- Etc.

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 Premium Outbound Filtering: Customers using outbound premium email filtering services from Proofpoint must **not** connect directly to these services from their devices or workstations.

4.6 Email Archival: Customers using Email Archival (provided through our partnership with Sonian) who are modifying their own Archival ingest settings must configure secure connections for the ingest of the messages into the archival system. Customers must also ensure that they do not send the results of archived email searches to non-compliant email addresses.

4.7 Premium Email Filtering: Customers with access to the Premium Email Filtering control panel at Proofpoint must ensure that any email delivery or email forwarding 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). Furthermore, Customers must not send outbound email messages containing ePHI from the Emergency Inbox feature, as these messages may not be encrypted.

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

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 for HIPAA compliance. LuxSci does not include the data in or passing though third party Widgets to be in its definition of possible 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.

www.luxsci.com
sales@luxsci.com
1.800.441.6612
LuxScientiae, Inc.
P.O. Box 326
Westwood, MA 02090

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-HIPAA-compliant users.

4.13 Opt Out: Customers who permit end users to opt out of outbound SecureLine email encryption on a per-message basis must ensure that their users are well trained in the identification of what constitutes ePHI and take on the responsibility for ensuring that their end users never misclassify ePHI-containing email as non-ePHI-containing email when opting out of encryption.

4.14 Training: Customers are required to train any individual who may be using a LuxSci HIPAA-compliant account in the proper usage thereof. This includes but is not limited to: (a) where ePHI can and cannot be located, (b) how to properly send unencrypted emails without ePHI, (c) what exactly constitutes ePHI, and (d) how to report breaches or errors. Proper training of these individuals is a requirement of HIPAA itself; be sure to incorporate proper usage of LuxSci with respect to your account in to your organization's HIPAA training and to perform this training whenever a new individual starts using LuxSci for the first time.

4.15 **SecureForm**: SecureForm permits Customer administrators to setup integrations which can cause ePHI in form data to flow from SecureForm to third-party services. It is Customer's responsibility to determine and ensure that either:

(a) the third-party service is owned by Customer and Customer certifies HIPAA compliance with respect to this ePHI, or
(b) Customer has a HIPAA Business Associate Agreement with the third-party service and that service will protect the ePHI in a manner which is HIPAA compliant and which will maintain the HIPAA compliance of the Customer, or
(c) HIPAA-compliant protections are not required by law for the ePHI after it arrives at the third-party service, or
(d) the ePHI will be protected by another organization that falls under the scope of HIPAA law but which is not a HIPAA Business Associate of Customer, or
(e) no ePHI will flow to the third-party service.

For example, if Customer chooses to send data from SecureForm to Slack then either:

(a) Customer must have a HIPAA-compliant account with Slack, or
(b) the Slack account must be HIPAA-compliant and owned by a Business Associate of Customer, or
(c) the Slack account must be owned by a person who has a right to view the ePHI and who has (for example) opted out of security through the Mutual Consent provisions of HIPAA, or
(d) the Slack channel is owned by another organization who assumes the HIPAA responsibilities for protecting the ePHI after delivery, or
(e) Customer ensures that no ePHI will be or can be in Slack by carefully choosing which data is sent there.

Any breaches of ePHI at the third-party service provider are the sole the responsibilities of Customer and/or the third-party service provider.

www.luxsci.com
sales@luxsci.com
1.800.441.6612
LuxScientiae, Inc.
P.O. Box 326
Westwood, MA 02090

5. Use of ePHI with LuxSci Services

As indicated in the Business Associate Agreement, *only certain types of data* are safeguarded with the appropriate level of security and privacy to comply with the HIPAA security requirements. *LuxSci strongly recommends that you train your personnel to enter ePHI only in the appropriate, secured, and designated areas.*

The following places are suitable for uploading and/or storing ePHI:

ePHI Recommended Locations

- **Email**: For sent or received email:
  - Email message body
  - Email attachments
- **WebAides**: all types
- **Widgets**: all types except for those created by third parties.
- **Database**: Hosted MySQL databases
- **SecureChat**
- **SecureVideo**
- **SecureText**
- **Files**: (stored in customer's FTP/Web hosting space)
  - **Shared servers**: ePHI may be stored in files if it is encrypted, cannot be decrypted with information in other readable files, and it is not publically accessible via customer Web sites. Even in such cases where the data is encrypted, the file name itself must not contain ePHI.
  - **Dedicated servers**: ePHI may be stored in files as long as it is not publically accessible via customer Web sites.

The following places are examples of locations NOT suitable for the inclusion of ePHI:

Never Include ePHI Here

- **Email headers***, including "From", "To", "Cc", "Reply-To", and "Subject".
- **Support tickets**
- **File names** of files stored on shared web servers
- **Widgets:** Custom widgets developed by third parties and/or which send data to/store data outside of the LuxSci environment.
- **Web Sites**
  - Pages not protected via TLS
  - Pages not protected by authentication / password access
  - Pages where individuals do not have unique access credentials
  - Pages do that do not include auditing and tracking of user activity, or which do not follow the other requirements of the HIPAA security rules

www.luxsci.com
sales@luxsci.com
1.800.441.6612
LuxScientiae, Inc.
P.O. Box 326
Westwood, MA 02090

(*) As the Subject, To, From, Cc, Bcc and other email metadata headers are required for delivery and validated by email integrity systems like DKIM, no email service provider will encrypt these items. While they may be encrypted during transit if TLS is used, they may be saved in plain text in log files of many different email servers across the Internet and may be sent in plain text in cases where TLS is not used. *Your organization needs to determine for itself if the mere act of sending an email message to a patient reveals ePHI, when the rest of the message is not ePHI or is encrypted*.

www.luxsci.com
sales@luxsci.com
1.800.441.6612
LuxScientiae, Inc.
P.O. Box 326
Westwood, MA 02090

Acceptance of Account Restrictions Agreement

*****Please sign using our online form at: http://luxsci.com/baa *****

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).

YES, I have read and agree with the Business Associate and Account Restrictions Agreements.

Customer Name: _____

Customer Title: _____

Organization Name: _____

Order Number: _____

_____
Customer Signature & Date

_____ _____
LuxSci Officer Name & Title LuxSci Signature & Date

www.luxsci.com
sales@luxsci.com
1.800.441.6612
LuxScientiae, Inc.
P.O. Box 326
Westwood, MA 02090