LUXSCI Be smart. Be secure.
Comprehensive, customizable
security since 1999

Medical Privacy

Version 2019.5.23

Business Associate Agreement

This Business Associate Agreement (the "Agreement") shall apply to the extent that the Lux Scientiae HIPAA Customer signee is a "Covered Entity" or "HIPAA Business Associate," as defined below. Execution of the Agreement does not automatically qualify either party as a "Covered Entity" or "HIPAA Business Associate" under law or regulation unless that party is considered a "Covered Entity" or "HIPAA Business Associate" under the applicable laws or regulations. This Agreement defines the rights and responsibilities of each of us with respect to Protected Health Information as defined in the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health (HITECH) provisions of the American Recovery and Reinvestment Act of 2009, the Omnibus Final Rule (as applied to 45 CFR Parts 160 and 164) and the regulations promulgated thereunder, as each may be amended from time to time (collectively, "HIPAA"). This Agreement shall be applicable only in the event and to the extent Lux Scientiae meets, with respect to you, the definition of a HIPAA Business Associate set forth at 45 C.F.R. Section §160.103, or applicable successor provisions.

1. Definitions

Capitalized terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the HIPAA Privacy Rule.

Specific definitions:

a. Agreement. "Agreement" or "Underlying Services Agreement" shall mean the Description of Services Ordered, the Lux Scientiae Master Services Agreement (https://luxsci.com/msa), any Lux Scientiae Addendum to the Master Services Agreement (including this Agreement), and the Lux Scientiae Acceptable Use Policy https://luxsci.com/aup), collectively.

b. Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean Lux Scientiae, Incorporated ("Lux Scientiae" or "LuxSci").

c. HIPAA Business Associate. "HIPAA Business Associate" shall mean an organization that has a HIPAA Business Associate Agreement with one or more "Covered Entities" or other "HIPAA Business Associates".

d. Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103.

e. HIPAA Customer. "HIPAA Customer" shall mean a customer of Lux Scientiae that is either (1) a Covered Entity, or (2) a HIPAA Business Associate, who has signed a Business Associate Agreement with Lux

Scientiae, and whose account security settings have been configured and locked down to meet the requirements of Section 2 of the Lux Scientiae Account Restrictions Agreement.

f. CFR. "CFR" shall mean the Code of Federal Regulations.

g. Disclosure. "Disclosure" of PHI means "the release, transfer, provision of, access to, or divulging in any other manner, of PHI outside the entity holding the information," as per 45 CFR 160.103.

h. Electronic Protected Health Information. "Electronic Protected Health Information" (ePHI) shall have the same meaning as the term "electronic protected health information" in 45 CFR 160.103, limited to the information created or received by Business Associate from or on behalf of HIPAA Customer.

i. Individual. "Individual" shall have the same meaning as the term "individual" in 45 CFR 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

j. Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

k. Protected Health Information. "Protected Health Information" (PHI) shall have the same meaning as the term "protected health information" in 45 CFR 160.103, limited to the information created or received by Business Associate from or on behalf of HIPAA Customer.

l. Required by Law. "Required by Law" shall have the same meaning as the term "required by law" in 45 CFR 164.103.

m. Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

n. Security Incident. "Security incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

o. Security Rule. "Security Rule" shall mean those requirements of the 45 CFR Part 164.308, 164.310, 164.312, 164.314, and 164.316.

p. Use. "Use" of PHI shall mean "the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information," as per 45 CFR 160.103.

q. HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

r. End User. A person who has a username and password to login as a user of HIPAA Customer's LuxSci account. I.e., End Users may have email or other services hosted at LuxSci through HIPAA Customer or they may be administrators of HIPAA Customer's account.

2. What is Safeguarded by Business Associate

There are many kinds of data that HIPAA Customer may store in or transmit through Business Associate's services. Business Associate cannot know specifically which information is ePHI and which is not, though Business Associate is required to ensure the security and privacy of all HIPAA Customer's ePHI as per the Security and Privacy Rules. Business Associate uses a blanket definition to consider certain classes of data to be "potential ePHI" so it can ensure the security and privacy of actual ePHI in a straight forward and consistent manner.

Data *will not be considered potential ePHI* if:

- It is not created or received by Business Associate from, for, or on behalf of HIPAA Customer.
- It is created or received by Business Associate from or on behalf of a free trial account.
- It is created or received by Business Associate from or on behalf of an End User that is not considered HIPAA-compliant by Business Associate (e.g. the user is part of a domain that is not considered HIPAA compliant by Business Associate, even though other domains in HIPAA Customer's account are considered HIPAA compliant).
- The HIPAA Customer or one or more of its End User(s) have specified that the data does not contain ePHI (e.g. by explicitly opting out of the use of email encryption and certifying that no ePHI is contained in a message).

Business Associate otherwise will treat the following classes of data as "potential ePHI" for the purposes of ensuring the security and privacy of that data as per the Security and Privacy Rules:

a. *Sent Email*. The content of all sent outbound email messages

   i. The combination of the subject, sender address, recipient addresses, and other email header metadata is not considered potential ePHI, though they are covered by Business Associate's privacy and non-disclosure policies.

   ii. Sent Email includes only email messages sent by HIPAA Customer from Business Associate's WebMail, API, user-authenticated SMTP services (including Premium High Volume), and SecureForm services.

   iii. Sent Email does not include email messages "sent" as a result of inbound email processing rules, such as email forwards, email notices, etc. Those are classified as "Received Email" messages.

b. *Received Email*. The content of received inbound email messages

- i. *The subject, sender address, recipient addresses, and other email header metadata is not considered potential ePHI, though they are covered by Business Associate's privacy and non-disclosure policies.*
- ii. *Notices to pick up secure messages on a web site are not themselves considered potential ePHI.*

c. *WebAides.* The content of WebAides Apps

- i. *This includes: WebAide Documents, Blogs, Address Books, Calendars, Tasks, Links, Notes, Passwords, and any other WebAides that may be introduced.*
- ii. *This applies to all WebAide content including comments, notes, and file attachments*
- iii. *This applies whether or not the WebAide content has been encrypted using optional PGP encryption by HIPAA Customer.*

d. *Widgets*. The content of Widgets

- i. *This includes: Notepad widgets, WebAide widgets, and all other widgets that do not otherwise indicate that they should not be used for ePHI.*
- ii. *This excludes: Custom widgets created by HIPAA Customer or third parties.*

e. *Databases*. The content of any LuxSci-hosted MySQL databases that the customer may be using for web hosting or SecureForm data storage.

- i. *This applies even if HIPAA Customer has not encrypted the ePHI in the database.*

f. *File Storage*. Applies to files stored on HIPAA-customer's web hosting/FTP file space

- i. *This includes all files stored in this space on servers dedicated to HIPAA Customer*
- ii. *This includes PGP- or SSL-encrypted files stored in this space on servers that HIPAA Customer shares with other Customers.*

g. Spotlight Mailer. Including:

- *i.* The content of email templates, contact and subscriber lists, campaigns, and other data that can be stored on behalf of HIPAA Customer in the Spotlight Mailer system.
- *ii.* Excludes images uploaded to be included in email messages sent by Spotlight Mailer.

h. SecureChat Messages. Including:

- i. *The content (participants, conversation subject, individual messages, and file attachments) of all conversations in the SecureChat system.*

i. *SecureText Messages.* The content of all sent SecureText messages

i. *As with secure email, the combination of the subject, sender address, recipient address(es), and other metadata is not considered potential ePHI, though they are covered by Business Associate's privacy and non-disclosure policies.*

ii. *Notices to pick up secure messages on a web site are not themselves considered potential ePHI.*

j. *SecureVideo.* Including:

i. *All traffic through the SecureVideo application (data in motion). I.e. video, chat, screen sharing, and file transfer activity.*

ii. *Information stored in the SecureVideo web application. Including session notes, saved session videos, schedules, and contact lists.*

While Business Associate safeguards all data in these classes as "PHI" with respect to its security and privacy policies, a "Breach" caused by a Use or Disclosure of PHI other than as permitted or required by this Agreement or as permitted or Required by Law *will only be construed to occur if the data Used or Disclosed was actually PHI as defined in Section 1*.

3. Obligations and Activities of Business Associate

a. Business Associate agrees to not Use or Disclose PHI other than as permitted or required by this Agreement or as permitted or required by law. In particular, Business Associate has obligations under the HIPAA HITECH Act and agrees to abide by those requirements.

b. Business Associate agrees to use appropriate safeguards to prevent Use or Disclosure of the PHI other than as provided for by this Agreement. In particular, Business Associate agrees to comply with the Privacy Rule and Security Rule with respect to all data considered potential ePHI per Section 2, subject to the caveats in 3c, which are created at, received by, maintained at, or transmit through Business Associate services.

c. Business Associate provides many mechanisms by which HIPAA Customer can safeguard PHI, which, when properly utilized by HIPAA Customer, will ensure compliance with the provisions of the Privacy Rule and the Security Rule. As the use of Business Associate's services with respect to PHI varies significantly from one HIPAA Customer to another, Business Associate by default does not automatically lock down the security of information storage and transfer to the *maximum* degree possible and does not require that HIPAA Customer purchase or employ all possible services available to it to do so, as that would not be appropriate for many HIPAA Customers. Business Associate will, upon request, advise the HIPAA Customer as to the most appropriate measures it should take with regards to Business Associate's services in order to ensure compliance with the Privacy Rule and the Security Rule, and will assist HIPAA Customer in taking those measures. *However, it is the sole responsibility of HIPAA Customer to choose and utilize those optional security measures that it deems appropriate for its business practices with respect to Business Associate and to utilize those services properly.*

d. Business Associate agrees to mitigate, to the extent reasonably practicable, any harmful effect that is known to Business Associate of a Use or Disclosure of PHI by Business Associate or its agents or subcontractors in violation of the requirements of this Agreement.

e. Business Associate agrees to report to HIPAA Customer any Use or Disclosure of PHI not provided for by this Agreement of which it becomes aware, or any Security Incident of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410. Notwithstanding the foregoing, this shall serve as Business Associate's notice to HIPAA Customer for the ongoing occurrence of unsuccessful attempts at unauthorized access, Use, Disclosure, modification, or destruction of PHI, or unsuccessful attempts at interference with system operations in an information system, such as "pings" on a firewall.

f. In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, Business Associate agrees to ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the Business Associate agree to substantially similar restrictions, conditions, and requirements that apply to the Business Associate with respect to such information.

g. All PHI maintained by Business Associate for HIPAA Customer will be available to HIPAA Customer in a time and manner that reasonably allows HIPAA Customer to comply with the requirements under 45 CFR § 164.524. Business Associate shall not be obligated to provide any such information directly to any Individual or person other than HIPAA Customer.

h. All PHI and other information maintained by Business Associate for HIPAA Customer will be available to HIPAA Customer in a time and manner that reasonably allows you to comply with the requirements under 45 CFR § 164.526.

i. Business Associate agrees to document such Disclosures of PHI and information related to such Disclosures that is it aware of as would be required for HIPAA Customer or respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR 164.528. This provision covers the actions of Business Associate with respect to explicit Disclosure of PHI*; it does not cover Disclosures that may result from inappropriate choices of security settings or inappropriate usage of Business Associate's services by HIPAA Customer.*

j. You acknowledge that Business Associate is not required by this Agreement to make Disclosures of PHI to Individuals or to any person other than HIPAA Customer, and that Business Associate does not, therefore, expect to maintain documentation of such Disclosure as described in 45 CFR § 164.528. In the event that Business Associate does make such Disclosure, it shall document the Disclosure as would be required for you to respond to a request by an Individual for an accounting of Disclosures in accordance with 45 CFR §164.528, and shall provide such documentation to you promptly on your request.

Business Associate agrees to keep any electronic records of all such Disclosures of PHI for a period of at least 6 years. This includes manual records of explicit/manual Disclosers by staff and automated records such as audit trails and log files.

k. Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set that the HIPAA Customer directs or agrees to pursuant to 45 CFR §164.526 at the request of HIPAA Customer or an Individual.

l. Business Associate agrees to make internal practices, books, and records, including policies and procedures and PHI, relating to the Use and Disclosure of PHI received from, or created or received by Business Associate on behalf of, HIPAA Customer available to the Secretary, in a time and manner designated by the Secretary, for purposes of the Secretary determining HIPAA Customer or Business Associate's compliance with the Privacy or Security Rules.

m. Business Associate agrees to abide by requirements not to Disclose PHI to insurers or other Health Plans if the patient pays for the service in full and requests confidentiality. It is the obligation of the HIPAA Customer to notify Business Associate of such cases.

n. Business Associate agrees to provide to HIPAA Customer, in the timely manner, information collected in accordance with this Business Associate Agreement, to permit HIPAA Customer to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with the HIPAA Rules. If an Individual makes a request for an accounting directly to Business Associate, Business Associate shall notify HIPAA Customer of the request in a timely manner so that HIPAA Customer may send the response to the Individual.

o. If Business Associate explicitly agrees to carry out and carries out a specific obligation under the HIPAA Privacy Rule on the behalf of HIPAA Customer, Business Associate agrees to comply with the requirements of the Privacy Rule with respect to the performance of that obligation.

4. Permitted Uses and Disclosures by Business Associate

Except as otherwise limited in this Agreement or other portion of the Agreement, Business Associate may Use or Disclose PHI to perform functions, activities, or services for, or on behalf of, HIPAA Customer as specified in the Agreement, provided that such Use or Disclosure would not violate the Privacy Rule if done by you.

Business Associate's services include the transmission of material over email, web sites, and other means. Business Associate provides the means to ensure that PHI is encrypted so that it will not be Disclosed in ways that would violate the Privacy Rule. As per obligation 3c and 6a, it is up to HIPAA Customer to use the appropriate optional services to ensure the appropriate level of security for the PHI that travels through or is stored in Business Associate's services.

5. Specific Use and Disclosure Provisions.

Except as otherwise limited in this Agreement or other portion of the Agreement, Business Associate may:

a. Use PHI for the proper management and administration of Business Associate or to carry out its legal responsibilities;

b. Disclose PHI for the proper management and administration of Business Associate, provided that disclosures are (i) Required By Law, or (ii) Business Associate obtains reasonable assurances from the person to whom the information is Disclosed that it will remain confidential and used or further Disclosed only as Required By Law or for the purpose for which it was Disclosed to the person, and the person will notify Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached; and

c. Use PHI to report violations of law to appropriate Federal and State authorities, consistent with §164.502(j)(1).

6. Obligations of HIPAA Customer

a. HIPAA Customer is obliged to utilize Business Associate's services in a way that ensures that HIPAA Customer is in compliance with the Privacy Rule.

b. HIPAA Customer shall notify Business Associate of any limitation(s) in its notice of privacy practices of HIPAA Customer in accordance with 45 CFR 164.520, to the extent that such limitation may affect Business Associate's Use or Disclosure of PHI.

c. HIPAA Customer shall notify Business Associate of any changes in, or revocation of, permission by Individual to Use or Disclose PHI, to the extent that such changes may affect Business Associate's Use or Disclosure of PHI.

d. HIPAA Customer shall notify Business Associate of any restriction to the Use or Disclosure of PHI that HIPAA Customer has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Business Associate's Use or Disclosure of PHI.

e. HIPAA Customer shall not request Business Associate to Use or Disclose PHI in any manner that would not be permissible under the Privacy Rule if done by HIPAA Customer.

f. HIPAA Customer agrees not to use Business Associate's services for the transmission or storage of ePHI except in modes or locations actively safeguarded by Business Associate as potential ePHI, as defined in

Section 2.

g. HIPAA Customer agrees to notify Business Associate of any of its users whose PHI should not be Disclosed to insurers or Health Plans due to the fact that they pay in full for their own insurance and have requested confidentiality.

7. Term and Termination

a. Term. The Term of this Agreement shall be effective as of the date when HIPAA Customer signs this Agreement and it is accepted by Lux Scientiae, and shall terminate when all of the PHI provided by HIPAA Customer to Business Associate, or created or received by Business Associate on behalf of HIPAA Customer, is destroyed or returned to HIPAA Customer, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.

b. Termination for Cause. Upon HIPAA Customer 's knowledge of a material breach by Business Associate, HIPAA Customer shall either:

1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement if Business Associate does not cure the breach or end the violation within thirty (30) calendar days;

2. Immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible; or

3. If neither termination nor cure is feasible, HIPAA Customer shall report the violation to the Secretary.

In the case of legitimate Termination for Cause, HIPAA Customer may also terminate its accounts with Business Associate without regard to any time remaining on HIPAA Customer's account contracts, though any amounts due to Business Associate at that time will become immediately due. Additionally, Businesses Associate may immediately terminate this Business Associate Agreement and the Customer’s account upon notice to HIPAA Customer if the HIPAA Customer fails to meet its HIPAA obligations.

c. Effect of Termination.

1. Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy, within 90 days of termination, all PHI

received from HIPAA Customer, or created or received by Business Associate on behalf of HIPAA Customer. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI after this time.

2. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall extend the protections of this Agreement to such PHI and limit further Uses and Disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

8. Miscellaneous

a. Regulatory References. A reference in this Agreement to a section in the Privacy Rule or Security Rule means the section as in effect or as amended.

b. Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for HIPAA Customer to comply with the requirements of the Privacy Rule, the Security Rule, the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, and all subsequent laws and regulations bearing on the subject matter of this Agreement.

c. Survival. The respective rights and obligations of Business Associate under Section 6.c of this Agreement shall survive the termination of this Agreement.

d. Interpretation. Any ambiguity in this Agreement shall be resolved to permit HIPAA Customer to comply with the Privacy Rule and Business Associate to comply with the Privacy and Security Rules. With respect to each Parties obligations under 45 CFR Parts 160 and 164, the provisions of this Business Associate Agreement shall prevail over any provisions in the Underlying Services Agreement between the Parties that may conflict or appear inconsistent.

Acceptance of Business Associate Agreement

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

Customer Name: Clint Reed

Customer Title: Owner

Organization Name: PMU Sign LLC

Order Number: 207008

____
Customer Signature & Date

Erik Kangas, Ph.D.
CEO
____
LuxSci Officer Name & Title

Erik Kangas October 4, 2019
____
LuxSci Signature & Date

Account Restrictions Agreement [ARA]

Required by LuxSci HIPAA Accounts

Version 2019.02.15

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 fully 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.

2.2 Password Strength: All passwords used by all users to access LuxSci servers must be "strong". This means that, at a minimum, 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 the 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.

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 a sufficiently secure version of 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 a way that appears "normal."

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

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. Questions and answers are needed for Escrow when SecureSend Recipient Authentication (3.5) is not enabled.

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 their login credentials 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 do 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.

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 in writing, 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.**

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, as that will bypass outbound email encryption.

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 or exports to non-compliant email addresses or storage locations.

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 through 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.

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 email 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.

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/MariaDB 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”.
- **LuxSci customer 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

(*) 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*.

Acceptance of Account Restrictions 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).

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

Customer Name: Clint Reed

Customer Title: Owner

Organization Name: PMU Sign LLC

Order Number: 207008

Customer Signature & Date

LuxSci Officer Name & Title

Erik Kangas October 4, 2019

LuxSci Signature & Date

Customer Signature [Name: Clint Reed; Date:October 4, 2019]