Medical Privacy

Version 2018.12.03

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

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" shall mean the Description of Services Ordered, the Lux Scientiae Master Services Agreement (https://luxsci.com/extranet/msa.html), any Lux Scientiae Addendum to the Master Services Agreement (including this Agreement), and the Lux Scientiae Acceptable Use Policy https://luxsci.com/extranet/aup.html or https://luxsci.com/extranet/hipaa-bulk-email-aup.html as applicable), 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.

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

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

o. 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.

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

q. 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.

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

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.*

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

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.*

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

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.

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

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, including breaches of unsecured protected health information as required at 45 CFR 164.410. Such notice will be made within 2 business days of the discovery of the breach.

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 vendors or 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 consider any amendment(s) to PHI stored on the Business Associate's servers in accounts owned by HIPAA Customer at the request of HIPAA Customer or an Individual, and in the time and manner agreed upon by Business Associate and HIPAA Customer. Such amendments and their terms must be negotiated and agreed upon by Business Associate and HIPAA Customer before they

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

will be implemented.

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, within 30 days of a verified request, 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 within three business (3) days of such request 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 indemnify and hold harmless Business Associate, its directors, officers, shareholders, parents, subsidiaries, affiliates, and agents, from and against all losses, expenses, damages and costs, including reasonable attorneys' fees, resulting from HIPAA Customer's failure to fulfill its

obligations under this Agreement and to use Business Associate's services in such a manner as to prevent the unauthorized disclosure of PHI.

h. 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 the time specified by HIPAA Customer;

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, with or without notice, terminate this Business Associate Agreement and the Customer's account 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 provide to HIPAA Customer notification of the conditions that make return or destruction infeasible. If return or destruction of 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.

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

Acceptance of Business Associate Agreement

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

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