



## Medical Privacy

Version 2010.06.23 - Standard

### Business Associate Agreement

This Business Associate Agreement (the "Agreement") shall apply to the extent that the Lux Scientiae Customer signee is a "Covered Entity," 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, 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 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 Service Description, any the Master Services Agreement, any Lux Scientiae Addendum to the Master Services Agreement (including this Agreement), and the Acceptable Use Policy, collectively.
- b. Business Associate. "Business Associate" shall mean Lux Scientiae, Incorporated ("Lux Scientiae").
- c. HIPAA Business Associate. "HIPAA Business Associate" shall mean an organization that has a HIPAA Business Associate Agreement with one or more "Covered Entities."
- d. Covered Entity. "Covered Entity" shall mean a client of Lux Scientiae that is (1) a health plan, (2) a health care clearinghouses, or (3) a health care provider who electronically transmits any health information in connection with transactions for which the U.S. Department of Health and Human Services has adopted standards. In this agreement, the term "Covered Entity" will also be extended to include a client of Lux Scientiae who is a "HIPAA Business Associate."
- e. CFR. "CFR" shall mean the Code of Federal Regulations.
- f. 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.
- g. 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 Covered Entity.

- h. 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).
- i. 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.
- j. 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 Covered Entity.
- k. Required by Law. “Required by Law” shall have the same meaning as the term “required by law” in 45 CFR 164.103.
- l. Secretary. “Secretary” shall mean the Secretary of the Department of Health and Human Services or his designee.
- m. Security Rule. “Security Rule” shall mean those requirements of the 45 CFR Part 164.308, 164.310, 164.312, 164.314, and 164.316.
- n. 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.

## 2. What is considered ePHI by Business Associate.

There are many kinds of data that a Customer may store in or pass through Business Associate’s services. As Business Associate cannot know specifically which information ePHI and which is not, though Business Associate is required to ensure the security and privacy of all covered Entity’s ePHI as per the Security and Privacy Rules, Business Associate uses a blanket definition to consider certain classes of data to be “ePHI” so it can ensure the security and privacy of actual ePHI in a straight forward and consistent manner. Business Associate will treat the following classes of data as “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 email messages
  - i. *The subject, sender address, recipient addresses, and other email header metadata is not considered ePHI, though they are covered by Covered Entity’s standard privacy and non-disclosure policies.*
  - ii. *Sent Email includes only email messages sent by Covered Entity from Business Associate’s WebMail or user-authenticated SMTP 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.*



- b. *Received Internal or Encrypted Email.* The content of all received secure email messages
  - i. *The subject, sender address, recipient addresses, and other email header metadata is not considered ePHI, though they are covered by Covered Entity's standard privacy and non-disclosure policies.*
  - ii. *"Secure messages" are those that are transmitted from the sender's email server(s)*
    - 1. *Over a TLS-encrypted SMTP connection, or*
    - 2. *PGP-encrypted, or*
    - 3. *S/MIME-encrypted*
    - 4. *Notices to pickup secure messages on a web site are not themselves ePHI.*
- c. *WebAides.* The content of WebAides
  - 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 Covered Entity.*
- 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 Covered Entity or third parties.*
- e. *Databases.* The content of any MySQL databases that the customer may be using for web hosting.
  - i. *This applies even if Covered Entity has not PGP-encrypted the ePHI in the database.*
- f. *File Storage.* Applies to files stored on Covered Entity's web hosting/FTP file space
  - i. *This includes all files stored in this space on servers dedicated to the Covered Entity*
  - ii. *This includes PGP- or SSL-encrypted files stored in this space on servers that the Covered Entity shares with other Customers.*

While Business Associate treats 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.
- 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 ePHI per Section 2, subject to the caveats in 3c.
- c. Business Associate provides many mechanisms by which the Covered Entity can safeguard PHI, which, when properly utilized by Covered Entity, 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 Covered Entity 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 Covered Entity purchase or employ all possible services available to it to do so, as that would not be appropriate for many Covered Entities. Business Associate will, upon request, advise the Covered Entity 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 the Covered Entity in taking those measures. *However, it is the sole responsibility of the Covered Entity to choose and utilize those optional security measures that it deems appropriate for its business practices with respect to Business Associate.*
- 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 Covered Entity any Use or Disclosure of PHI not provided for by this Agreement of which it becomes aware. Such notice will be made within 60 days of the discovery of the breach as per SEC 13302 of the American Recovery and Reinvestment Act of 2009.
- f. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by Business Associate on behalf of Covered Entity, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.
- g. All PHI maintained by Business Associate for Covered Entity will be available to Covered Entity in a time and manner that reasonably allows Covered Entity 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 Covered Entity.
- h. All PHI and other information maintained by Business Associate for Covered Entity will be available to Covered Entity 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 it is aware of as would be required for Covered Entity 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 Covered Entity.*
- j. You acknowledge that Business Associate is not required by this Agreement to make Disclosures of PHI to Individuals or any person other than Covered Entity, 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.
- k. Business Associate agrees to consider any amendment(s) to PHI stored on the Business Associate's servers in accounts owned by Covered Entity at the request of Covered Entity or an Individual, and in the time and manner agreed upon by Business Associate and Covered Entity. Such amendments and their terms must be negotiated and agreed upon by Business Associate and Covered Entity before they 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, Covered Entity available to the Secretary, within 30 days of a verified request, for purposes of the Secretary determining Covered Entity or Business Associate's compliance with the Privacy or Security Rules.

## 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, Covered Entity 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 Covered Entity 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 Covered Entity

- a. Covered Entity is obliged to utilize Business Associate's services in a way that ensures that Covered Entity is in compliance with the Privacy Rule.
- b. Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR 164.520, to the extent that such limitation may affect Business Associate's Use or Disclosure of PHI.
- c. Covered Entity 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. Covered Entity shall notify Business Associate of any restriction to the Use or Disclosure of PHI that Covered Entity 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. Covered Entity 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 Covered Entity.
- f. Covered Entity agrees not to use Business Associate's services for the transmission or storage of ePHI, except for that ePHI which meets one or more of the classes of ePHI supported by Business Associate as defined in Section 2.
- g. Covered Entity 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 Covered Entity's failure to fulfill its obligations under this Agreement to use Business Associate's services in such a manner as to prevent the unauthorized disclosure of PHI.



## 7. Term and Termination

- a. Term. The Term of this Agreement shall be effective as of the date when Covered Entity signs this Agreement and it is accepted by Lux Scientiae, and shall terminate when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, 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 Covered Entity's knowledge of a material breach by Business Associate, Covered Entity 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 Covered Entity;
  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, Covered Entity shall report the violation to the Secretary.

In the case of legitimate Termination for Cause, Covered Entity may also terminate its accounts with Business Associate without regard any time remaining on Covered Entity's account contracts, though any amounts due to Business Associate at that time will become immediately due.

- 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 Covered Entity, or created or received by Business Associate on behalf of Covered Entity. 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 Covered Entity 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 Covered Entity 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 Covered Entity to comply with the Privacy Rule and Business Associate to comply with the Privacy and Security Rules.

Acceptance of Business Associate Agreement

Accepted by:

\_\_\_\_\_
Customer Name & Title

\_\_\_\_\_
LuxSci Officer Name & Title

\_\_\_\_\_
Signature & Date

\_\_\_\_\_
Signature & Date

Account or Order #: \_\_\_\_\_

**All pages are required to be returned to LuxSci.**

Fax: 413-332-0598

Email: sales@luxsci.us

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