

# BUSINESS ASSOCIATE AGREEMENT (“BAA”)

November 17, 2016 Revision

This BAA can be found at

<https://www.thinksis.com/legal>

This Business Associate Agreement (“Agreement”) is made effective \_\_\_\_\_ (“Effective Date”) between \_\_\_\_\_ (“Covered Entity”) and Software Information Systems, LLC (“SIS or Business Associate”). The terms of this Agreement will be upheld such that said terms apply to the service or product provided by Business Associate to Covered Entity to which will be limited to technology consultant or service provider.

## RECITALS

- A. Covered Entity is a covered entity under the Health Insurance Portability and Accountability Act of 1996, as amended (“HIPAA”), including the HIPAA Rules (as defined below), and the Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act of 2009 (the “HITECH Act”).
- B. Covered Entity and SIS have entered into the SIS Statement of Work (the “SOW”) pursuant to which SIS will provide certain services to Covered Entity and, pursuant to the SOW, SIS may receive, maintain or have access to Electronic Protected Health Information (as defined below) dependent upon the type of services provided in fulfilling its responsibilities under the SOW.
- C. As a service provider or technology consultant to Covered Entity as described above, SIS may be considered a “Business Associate” of Covered Entity as defined in the HIPAA Rules. The HIPAA Rules include the Standards for Privacy of Individually Identifiable Health Information (the “Privacy Rule” at 45 CFR Part 160 and Part 164, Subparts A and E), the Standards for Security of Electronic Protected Health Information (the “Security Rule” at 45 CFR Parts 160 and 164, Subpart C), Breach Notification for Unsecured Protected Health Information (the “Breach Notification Rule” at 45 CFR Parts 160 and 164), and the Enforcement Rules at 45 CFR Part 160, Subparts C-E, as each of the foregoing may be amended or supplemented.
- D. SIS and Covered Entity are both committed to complying with the HIPAA Rules, and acknowledge that each has certain obligations to maintain the privacy and security of PHI.

NOW THEREFORE, Covered Entity and Business Associate agree within the scope defined by the SOW and subsequent terms as follows:

### 1. DEFINITIONS.

- 1.1. **Breach** shall mean the acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule that compromises the security or privacy of the PHI as defined, and subject to the exceptions set forth, in 45 CFR Section 164.402.

- 1.2. **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 Software Information Systems, LLC.
- 1.3. **Covered Entity** shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean \_\_\_\_\_.
- 1.4. **HIPAA Rules** shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164..
- 1.6. **Individual** shall have the same meaning as the term "individual" in 45 CFR 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).
- 1.7. **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.
- 1.8. **Protected Health Information** shall have the same meaning as the term "protected health information" in 45 CFR 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.
- 1.9. **Required by Law** shall have the same meaning as the term "required by law" in 45 CFR 164.501.
- 1.10. **Secretary** shall mean the Secretary of the Department of Health and Human Services or his designee.
- 1.11. **Security Rule** shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Part 160 and Part 164, Subparts A and C.

All other capitalized terms not defined herein shall have the meanings assigned in the Privacy Rule, the Security Rule and the HITECH Act.

## **2. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE.**

- 2.1. **Limitations on Use or Disclosure.** Business Associate agrees to not use or further disclose Protected Health Information other than as permitted or required by the Agreement or as required by Law.
- 2.2. **Safeguards.** Business Associate agrees to use reasonable and appropriate administrative, physical, and technical safeguards, and comply with the applicable requirements of Subpart C of 45 CFR Part 164 with respect to electronic Protected Health Information that it creates, receives, maintains or transmits, to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

- 2.3. Mitigation. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.
- 2.4. Reporting. Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware, including (1) any use and/or disclosure of Protected Health Information that is not permitted or required by this Agreement of which Business Associate becomes aware; (2) breaches of unsecured Protected Health Information as required at 45 CFR 164.410, and (3) any security incident of which it becomes aware Notification of a Breach will be made without unreasonable delay, but in no event more than thirty (30) calendar days after discovery of a Breach. Taking into account the level of risk reasonably likely to be presented by the use, disclosure, security incident, or Breach, the timing of other reporting will be made consistent with Business Associate and Customer's legal obligations. Business Associate's obligation to report under this Section is not and will not be construed as an acknowledgement by Business Associate of any fault or liability with respect to any use, disclosure, security incident, or Breach.
- 2.5. Subcontractors. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information 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, in accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2).
- 2.6. Access. If Business Associate maintains Protected Health Information in a Designated Record Set for Covered Entity, then Business Associate agrees to provide access when feasible, at the request of Covered Entity, within fifteen (15) days to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR 164.524.
- 2.7. Amendment. If Business Associate maintains Protected Health Information in a Designated Record Set for Covered Entity, then Business Associate, at the request of the Customer, shall make available such Protected Health Information to the Customer for amendment and incorporate any reasonably requested amendment in the Protected Health Information in accordance with CFR 164.526 of the Privacy Rule.
- 2.8. Disclosure to the Secretary. Business Associate agrees to make internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Covered Entity, or at the request of the Covered Entity to the Secretary, in a time and manner designated by the Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

- 2.9. Accounting of Disclosures. Business Associate, at the request of Covered Entity, agrees to within fifteen(15) days make available to Covered Entity such relating to Disclosures made by Business Associate as required by Covered Entity to make any requested accounting of disclosures of Protected Health Information in accordance with CFR 164.528.
- 2.10. Performance of a Covered Entity's Obligations. To the extent Business Associate is to carry out a Covered Entity obligation under the Privacy Rule, Business Associate shall comply with the requirements of the Privacy Rule that apply to Covered Entity in the performance of such obligation.
- 2.11. Data Ownership. Business Associate acknowledges that Business Associate has no ownership rights with respect to the PHI.

### **3. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE.**

- 3.1. General Use and Disclosure Provisions: Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, Covered Entity for the purposes discussed in this section, if such use or disclosure of Protected Health Information would not violate the Privacy Rule if done by Covered Entity, for the purpose of performing the Service Agreement.
- 3.2. Specific Use and Disclosure Provisions:
  - 3.2.1. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
  - 3.2.2. Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are required by law, or 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 notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
  - 3.2.3. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 42 CFR 164.504(e)(2)(i)(B).

### **4. OBLIGATIONS OF COVERED ENTITY.**

- 4.1. Covered Entity shall provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with 45 CFR 164.520, as well as any changes to such notice.
- 4.2. Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.
- 4.3. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, if such changes affect Business Associate's permitted or required uses and disclosures.
- 4.4. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR 164.522.
- 4.5. Permissible Requests by Covered Entity: Covered entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.
- 4.6. Covered Entity acknowledges that Covered Entity is accountable for compliance with the HIPAA Rules, and as such, has appropriately evaluated Business Associate as it relates to Business Associate providing product or services on behalf of Covered Entity.

## 5. TERM AND TERMINATION.

5.1 Term. The Term of this Agreement shall be effective as of the date first written above, and shall terminate when all of the Protected Health Information 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. Termination of this Agreement shall automatically terminate the Service Agreement.

5.2. Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall provide an opportunity for Business Associate to cure the breach or end the violation, and Covered Entity shall:

5.2.1. Terminate this Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity, or

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

5.2.3. If neither termination nor cure is feasible, Covered Entity will report the violation to the Secretary.

5.3. Effect of Termination.

- 5.3.1. Except as provided in the following paragraph, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity in accordance with State and Federal retention guidelines. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate and its subcontractors, if any, shall retain no copies of the Protected Health Information.
- 5.3.2. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of Protected Health information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.
- 5.3.3. In the event Covered Entity and Business Associate agree that Business Associate shall retain Protected Health Information after the termination of this Agreement, with respect to Protected Health Information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, Business Associate shall:
- 5.3.3.1. Retain only that Protected Health Information which is necessary for Business Associate to continue its proper management and administration to carry out its legal responsibilities;
  - 5.3.3.2. Return to Covered Entity the remaining Protected Health Information that Business Associate still maintains in any form;
  - 5.3.3.3. Continue to use reasonable and appropriate safeguards and comply with subpart C of 45 CFR part 164 with respect to electronic Protected Health Information to prevent use or disclosure of the Protected Health Information, other than as provided for in this Section for as long as Business Associate retains the Protected Health Information;
  - 5.3.3.4. Not to use or disclose the Protected Health Information retained by Business Associate other than for the purposes for which such Protected Health Information was retained and subject to the same conditions which applied prior to termination; and
  - 5.3.3.5. Return to Covered Entity the Protected Health Information retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

6. **MISCELLANEOUS.**

- 6.1. Regulatory References. A reference in this Agreement to a section in the HIPAA

Rules means the section as in effect or as amended, and for which compliance is required.

- 6.2. **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 and the Health Insurance Portability and Accountability Act, Public Law 104-191.
- 6.3. **Survival.** The respective rights and obligations of Business Associate under Section 5.3 of this Agreement shall survive the termination of this Agreement.
- 6.4. **Interpretation.** Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits compliance with the HIPAA Rules and other applicable laws.
- 6.5. **Indemnification.** Each party will indemnify, and hold harmless and defend the other party to this Agreement from and against any and all claims, losses, liabilities, costs, and other expenses (including reasonable attorneys' fees) incurred as a result of, or arising directly or indirectly out of or in connection with: (i) any misrepresentation, breach, or nonfulfillment of any duty on the part of either party under this Agreement; and (ii) any claims, demands, awards, judgments, actions and proceedings made by any person or organization arising out of or in any way connected with either party's negligent act or omission under this Agreement.
- 6.6. **No Third Party Beneficiaries.** Nothing expressed or implied in this Agreement is intended or shall be deemed to confer upon any person other than Covered Entity, Business Associate, and their respective successors and assigns, any rights, obligations, remedies or liabilities.
- 6.7. **Entire Agreement.** This Agreement is the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior agreements, negotiations, and communications of whatever type, whether written or oral, between the parties hereto with respect to the subject matter hereof, including any prior Agreement signed by the parties to comply with HIPAA, the HIPAA Privacy Regulations, the HIPAA Security Regulations and/or the HITECH Standards, if any. Except to the extent specifically amended hereby, the provisions of the Agreement shall remain unmodified, and the Agreement as amended hereby is confirmed as being in full force and effect.