



Business Associate Agreement

This Business Associate Agreement (“BAA”) is made effective as of the Effective Date, by and between HSS and Customer (referred to in this BAA as “Covered Entity”). Each of “HSS”, “Customer”, and “Effective Date” shall have the same meaning ascribed to them in the Service Agreement into which this BAA is incorporated.

WHEREAS, HSS and Covered Entity have entered into the Service Agreement whereby HSS provides or assists Covered Entity with a function or activity which may involve the use or disclosure of individually identifiable health information. In light of the foregoing, HSS and Covered Entity acknowledge that they are subject to the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), including the privacy and security regulations promulgated thereunder at 45 C.F.R. Parts 160 and 164, Subparts A and E (“Privacy Rule”), Subpart C (“Security Rule”), and Subtitle D of the Health Information Technology for Economic and Clinical Health Act (as incorporated in Title XIII of the American Recovery and Reinvestment Act of 2009) (“HITECH Act”), as amended from time to time (collectively referred to as the “HIPAA Standards”); and

WHEREAS, Covered Entity and HSS agree to enter into this BAA to ensure compliance with HIPAA Standards and any applicable state laws.

NOW, THEREFORE, in consideration of the mutual promises contained herein, the exchange of information pursuant to this BAA, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, Covered Entity and HSS agree as follows:

1. DEFINITIONS

Capitalized terms used in this BAA, but not otherwise defined shall have the same meaning ascribed to them in the HIPAA Standards. In the event of an inconsistency between the provisions of this BAA and mandatory provisions of HIPAA Standards, the HIPAA Standards in effect at the time shall control. Where provisions of this BAA are different than those mandated by HIPAA Standards, but are nonetheless permitted by such regulations, the provisions of this BAA shall control. Any reference herein to the HIPAA Standards or other federal or state regulation shall be a reference to such rule or regulation as in effect or as subsequently updated, amended or modified.

2. OBLIGATIONS OF HSS

HSS agrees to:

- a. Not use or disclose protected health information (hereinafter referred to as “PHI”, and as defined by the HIPAA Standards) other than as permitted or required by the Service Agreement or as Required by Law;
- b. Use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for by the Service Agreement;
- c. Report to Covered Entity any use or disclosure of PHI not provided for by the Service Agreement of which it becomes aware including, but not limited to, Breaches of Unsecured PHI as required by 45 C.F.R. §164.410 and any Security Incident of which it becomes aware, which Breaches and Security Incidents shall be reported in accordance with Section 5 of this BAA;
- d. In accordance with 45 C.F.R. §164.502(e)(1)(ii) and §164.308(b)(2), if applicable, ensure that any subcontracts that create, receive, maintain, or transmit PHI on behalf of HSS agree to the same restrictions, conditions, and requirements that apply to HSS with respect to such information;
- e. If HSS maintains information in a Designated Record Set, HSS shall:
 - i. Make available PHI in a Designated Record Set to Covered Entity as necessary to satisfy Covered Entity’s obligations under 45 C.F.R. §164.524; and



- ii. Make any amendment(s) to PHI in a Designated Record Set as directed by Covered Entity pursuant to 45 C.F.R. §164.526, or take other measures as necessary to satisfy Covered Entity's obligations under 45 C.F.R. §164.526;
- f. Maintain and make available information required to provide an accounting of disclosures to Covered Entity as necessary to satisfy Covered Entity's obligations under 45 C.F.R. §164.528;
- g. To the extent HSS is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 C.F.R. Part 164, comply with the requirements of Subpart E that apply to Covered Entity in the performance of such obligation(s);
- h. Make internal practices, books, and records available to the Secretary of the Department of Health and Human Services for purposes of determining compliance with the HIPAA Standards; and
- i. Retain all documentation required by this BAA for the applicable time periods required by the HIPAA Standards.

3. OBLIGATIONS OF COVERED ENTITY

Covered Entity shall:

- a. Privacy Practices. Provide HSS with the notice of privacy practices that Covered Entity provides to Individuals in accordance with 45 CFR 164.520, as well as any changes to such notice, to the extent that such change may affect the use or disclosure of PHI by HSS.
- b. Authorization Changes. Provide HSS with any changes in, or revocation of, permission by an Individual or the Individual's Personal Representative, to use or disclose PHI, if such changes affect the permitted or required uses and disclosures by HSS.
- c. Restrictions to Use or Disclosure. Notify HSS of any restriction to the use or disclosure of PHI that Covered Entity has agreed to as well as requests for confidential communication by alternative means and at alternative locations all in accordance with 45 CFR 164.522, to the extent such restrictions affect the use or disclosure of PHI by HSS.
- d. Permissible Requests. Not request HSS to use or disclose PHI in any manner that would not be permissible under the HIPAA Standards if done by Covered Entity.
- e. Amendments. Provide HSS with any amendments to PHI that Covered Entity has agreed to pursuant to 45 CFR 164.526, to the extent such amendments affect the use or disclosure of PHI by HSS.

4. PERMITTED USE AND DISCLOSURES BY HSS

- a. HSS may only use or disclose PHI as necessary to perform the Services set forth in the Service Agreement, provided such disclosures would not violate the HIPAA Standards if done by Covered Entity.
- b. HSS may use or disclose PHI as Required by Law.
- c. HSS will disclose only the Minimum Necessary PHI to perform its obligations under the Service Agreement.
- d. HSS may use or disclose PHI for the proper management and administration of HSS or to carry out the legal responsibilities of HSS, provided the disclosures are Required by Law, or HSS obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as Required by Law or for the purposes for which it was disclosed to the person, and the person notifies HSS of any instances in which it is aware in which the confidentiality of the information has been Breached.



5. REPORTING AND MITIGATING UNAUTHORIZED USES AND DISCLOSURES

- a. Reporting. HSS shall report, in writing, to Covered Entity's privacy officer, any unauthorized use or disclosure, including any Security Incident or Breach, as soon as practicable after HSS discovers such unauthorized use or disclosure. HSS shall be deemed to have discovered the unauthorized use or disclosure as of the first day on which the unauthorized use or disclosure is, or should reasonably have been, known to (i) HSS, or (ii) any employee, officer or other agent of HSS other than the individual committing the unauthorized use or disclosure. HSS shall not need to notify Covered Entity pursuant to this Section 5 if a Security Incident consists only of an unsuccessful attempt to access, use, modify or destroy information or an unsuccessful attempt to interfere with system operations. Further, HSS shall investigate the unauthorized use or disclosure and provide to Covered Entity, as soon as possible, all information Covered Entity may require to make notifications of Breach to individuals, or other persons or entities. HSS shall work in good faith with Covered Entity in addressing such unauthorized uses or disclosures.

The foregoing notwithstanding, if a law enforcement official notifies HSS that a notice to the Covered Entity of an unauthorized use or disclosure would impede a criminal investigation or cause damage to national security, HSS shall delay notifying the Covered Entity for the time period specified in the written notification from the law enforcement official. With respect to such Breach, if the law enforcement notification is oral, HSS shall document the request, including the identity of the official making the request, and delay notifying the Covered Entity but no longer than thirty (30) days from the date of the oral statement, unless a written statement is submitted by the law enforcement official during that time.

- b. Mitigation. HSS shall mitigate any harmful effect that is known to HSS of an unauthorized use or disclosure.
- c. Subpoenas. Unless otherwise prohibited by law, HSS shall provide Covered Entity with written notice of a subpoena served on HSS, in connection with PHI covered by this BAA, within three (3) business days of receipt of such subpoena.

6. TERM & TERMINATION

- a. Term. Subject to Section 6(b), the BAA shall be effective as of the Effective Date of the Service Agreement, and shall continue in effect while the Service Agreement remains in force, and thereafter with respect to those obligations intended to survive the termination of the Service Agreement and this BAA.
- b. Termination for Cause. As provided for under 45 C.F.R. §§164.504(e)(1)(ii) and 164.504(e)(2)(iii), either party may immediately terminate this BAA and the services being provided if such party determines that the other party has breached a material term of this BAA. Alternatively, and in the sole discretion of the non-breaching party, such party may choose to provide the breaching party with written notice of the breach and provide the breaching party with thirty (30) days to cure said breach. Failure by the breaching party to cure said breach within said thirty (30) day period shall be grounds for immediate termination of this BAA and the services being provided to Covered Entity.
- c. Obligation of HSS upon Termination. Upon termination of this BAA for any reason, HSS will return or destroy all PHI received from Covered Entity, or created or received by HSS on behalf of Covered Entity pursuant to 45 C.F.R. § 164.504(e)(2)(i), including PHI that is in the possession of subcontractors or agents of HSS. If HSS determines that the return or destruction of any PHI is infeasible (i.e., such PHI is necessary for HSS to continue its proper management and administration or to carry out its legal responsibilities), such PHI shall be retained by HSS and HSS shall extend the protections of this BAA to such retained PHI and limit any further uses and disclosures of such PHI to those purposes that make the return or destruction of such PHI not feasible, for so long as HSS maintains such PHI.



7. NOTICES

Any notice or other communication given pursuant to this BAA must be in writing and (i) delivered personally, (ii) delivered by nationally-recognized overnight express courier, or (iii) sent by registered or certified mail, postage prepaid, return receipt requested, to the addresses of the parties set forth in the Service Agreement. All such notices and communications shall be effective (a) if personally delivered, when delivered, (b) if sent by certified mail, three days after having been deposited in the mail, postage prepaid, or (c) if sent by overnight courier, one business day after having been given to such courier.

8. MISCELLANEOUS

- a. Interpretation. Any ambiguity in this BAA shall be resolved in favor of a meaning that permits the parties to comply with the HIPAA Standards.
- b. No Private Cause of Action/Third Party Beneficiaries. This BAA is not intended to and does not create a private cause of action by any individual, other than the parties to this BAA, as a result of any claim arising out of the breach of this BAA, the HIPAA Standards or other state or federal law or regulation relating to privacy or confidentiality. Nothing express or implied in this BAA is intended to confer, nor shall anything herein confer, upon any person other than the parties hereto any rights, remedies, obligations, or liabilities whatsoever.
- c. Amendment. This BAA shall only be amended or modified upon written consent of the parties. The parties agree to take such action as is necessary to amend this BAA from time to time as necessary for compliance with the requirements of HIPAA Standards and any other applicable law.
- d. Survival. The respective rights and obligations of HSS under Sections 2, 3, 4, 5, 8.b., 8.d., and 8.h. of this BAA shall survive the termination of this BAA.
- e. Waiver. Any waiver by either party of a breach of any provision of this BAA shall not operate as, or be construed as, a waiver of any subsequent breach or provision hereof.
- f. Assignability. This BAA and any rights, duties and obligations of the parties shall not be assigned by either party except upon written agreement signed by both parties.
- g. Binding Effect. This BAA is binding upon and shall inure to the benefit of the parties hereto and to their respective successors and permitted assigns.
- h. Severability. If any provisions of this BAA shall be declared invalid or illegal for any reason whatsoever, then notwithstanding such invalidity or illegality, the remaining terms and provisions of this BAA shall remain in full force and effect in the same manner as if the invalid or illegal provision had not been contained herein.
- i. Governing Law. To the extent not preempted by federal law, this BAA shall be interpreted, construed and governed by the laws of the State of New York, without regard to its conflicts of law principles. The parties agree that venue shall lie in Federal and State courts in the State of New York.
- j. Application of State Law. Where any applicable provision of state law relates to the privacy of health information and is not preempted by federal law, the parties shall comply with the applicable provision of state law.