**BUSINESS ASSOCIATE AGREEMENT TERMS**

This Addendum ("Addendum") is incorporated into and made part of the Agreement between SIGNATURE HEALTHCARE CORPORATION ("Covered Entity") and _____ ("Business Associate"), which was entered into as of _____ (the "Agreement").

Performing the Agreement requires Business Associate to be provided with, have access to, transmit, or create Protected Health Information or financial accounts that are subject to the federal law and regulations with respect to privacy, security, and breach notification: (1) Health Insurance Portability and Accountability Act of 1996 (HIPAA), including all pertinent regulations issued by the agencies of the United States Department of Health and Human Services (45 C.F.R. Parts 160 and 164), as amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act (HITECH Act), Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5) (collectively as "HIPAA Standards"), and/or (2) Identity Theft Red Flags rules published by the Federal Trade Commission at 61 C.F.R. part 681 ("Red Flags Rules"). In addition, performing the Agreement may also cause Business Associate to become a holder of Personal Information under Massachusetts state law (M.G.L. ch. 93H and related regulations) ("State Standards").

Both parties are committed to complying with the HIPAA Standards, Red Flags` Rules, and State Standards. This Agreement sets forth the terms and conditions under which Protected Health Information, Electronic Protected Health Information, or Personal Information that is provided by, or created or received by, the Business Associate from or on behalf of the Covered Entity, will be handled between the Business Associate and the Covered Entity and with third parties during the term of the Agreement and after its termination. In the event of an inconsistency between a term of the Agreement and this Addendum of Business Associate Agreement Terms, the terms of this Addendum shall govern in regard to the handling of Protected Health Information, Electronic Protected Health Information, and/or Personal Information.

The Parties agree as follows:

## 1. DEFINITIONS

**(a)** Protected Health Information or PHI shall have the same meaning as the term "protected health information" in 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

**(b)** Electronic Protected Health Information shall have the same meaning as the term "electronic protected health information" in 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

**(c)** Unsecured Protected Health Information or Unsecured PHI shall mean Protected Health Information that is not secured through the use of a technology or methodology specified by the Secretary in guidance or as otherwise defined in Section 13402(h) of the HITECH Act.

**(d)** Breach shall have the same meaning as the term "breach" has in Section 13400 of the HITECH Act and shall include the unauthorized acquisition, access, use, or disclosure of Protected Health Information, which compromises the security or privacy of such information.

**(e)** Privacy Rule shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. part 160, part 162 and part 164, subparts A and E.

**(f)** Security Rule shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. part 160 and part 164, subpart C.

**(g)** Secretary shall mean the Secretary of the Department of Health and Human Services or his/her designee.

**(h)** Personal Information shall mean the definition contained in the State Standards, as may be amended from time to time. At the time of the execution of this Addendum, Personal Information is defined in the State Standards as a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal Information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public. M.G.L. ch. 93H, § 1.

**(i)** Terms used, but not otherwise defined, in this Addendum shall have the same meaning as those terms in the HIPAA Standards, the HITECH Act, Red Flags Rules, or Massachusetts General Laws Chapter 93H, as applicable.

**(j)** The term Protected Health Information or PHI shall include both Protected Health Information and Electronic Protected Health Information ("ePHI"); however, ePHI shall be used when only Electronic Protected Health Information is being referenced.

## 2. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

**(a)** Business Associate agrees not to use or disclose Protected Health Information other than as permitted or required by the Agreement (including this Addendum) or as Required By Law.

**(b)** Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Addendum.

**(c)** 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 Addendum.

**(d)** Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Addendum of which it becomes aware. In event of a Breach of this Addendum by Business Associate or any of its officers, directors, employees, and subcontractors or agents, Business Associate shall immediately notify Covered Entity in accordance with the requirements of Section 13402 of HITECH Act.

**(e)** 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 Addendum to Business Associate with respect to such information.

**(f)** Business Associate agrees to provide access, within ten (10) days of receiving a written request from Covered Entity, 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 C.F.R. § 164.524, and any subsequent legislation or guidance regarding an Individual's right to access his or her Protected Health Information, including, but not limited to, the requirements of Sections 13405 of HITECH Act and the regulations thereunder.

**(g)** Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 C.F.R. § 164.526 and any subsequent legislation or guidance regarding and Individual's right to request amendment of his or her Protected Health Information within thirty (30) days of receiving a written request from Covered Entity.

**(h)** Business Associate agrees to implement administrative, physical, and technical safeguards ("Safeguards") that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI as required by 45 C.F.R. Part 164 Subpart C ("Security Rule") (see §164.314 (a)(2)(i)(A)).

**(i)** Business Associate agrees to ensure that any agent and subcontractor to whom Business Associate provides ePHI agrees to implement reasonable and appropriate safeguards to protect ePHI (see 45 C.F.R. §164.314 (a)(2)(i)(B)).

**(j)** Business Associate agrees to report promptly to Covered Entity any Security Incident of which Business Associate becomes aware (see 45 C.F.R. § 164.314 (a)(2)(i)(C)).

**(k)** Business Associate agrees to make its internal practices, books, and records, including policies and procedures, 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 within ten (10) days of receiving a written request from Covered Entity, or to the Secretary, in a time and manner designated by the Secretary, for purposes of the Secretary's determining Covered Entity's compliance with the Privacy Rule.

**(l)** Business Associate agrees to make its policies, procedures and documentation required by the Security Rule relating to the Safeguards for protecting ePHI that it creates, receives, maintains, or transmits on behalf of Covered Entity available to the Secretary for purposes of determining Covered Entity's compliance with the Security Rule.

**(m)** Business Associate agrees to document disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528 and any subsequent legislation or guidance regarding an Individual's right to an accounting of the disclosures of his or her Protected Health Information, including but not limited to, the requirements of Sections 13405 of HITECH Act and the regulations thereunder.

**(n)** Business Associate agrees to provide to Covered Entity, within thirty (30) days of receiving written notice, information collected in accordance with Section 2(m) of this Addendum to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528 and any subsequent legislation or guidance regarding an Individual's right to an accounting of the disclosures of his or her Protected Health Information, including, but not limited to, the requirements of Section 13405 of

HITECH Act and the regulations thereunder.

**3. REPORTING SECURITY INCIDENTS TO COVERED ENTITY**

Business Associate shall promptly notify Covered Entity of a Breach of Unsecured PHI following the first day on which Business Associate (or Business Associate's employee, officer or agent) knows of such Breach or following the first day on which Business Associate (or Business Associate's employee, officer or agent) should have known of such Breach. Business Associate's notification to Covered Entity hereunder shall:

**(a)** Be made to Covered Entity no later than sixty (60) calendar days after discovery of the Breach, except where a law enforcement official determines that a notification would impede a criminal investigation or cause damage to national security; and

**(b)** Include the individuals whose Unsecured Protected Health Information has been, or is reasonably believed to have been, the subject of a Breach.

**4. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE**

**(a)** Except as otherwise limited in this Addendum, Business Associate may use or disclose Protected Health Information 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 Covered Entity.

**(b)** Except as otherwise limited in this Addendum, Business Associate may disclose Protected Health Information for the proper management and administration or to carry out the legal responsibilities 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.

**(c)** Except as otherwise limited in this Addendum, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).

**(d)** Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. § 164.502(j)(1).

**(e)** Business Associate may de-identify any and all Protected Health Information created or received by Business Associate under this Agreement; provided, however, that the de-identification conforms to the requirements of the Privacy Rule and Business Associate notifies Covered Entity prior to creating de-identified Health Information. Such resulting de-identified information would not be subject to the terms of this Addendum.

**(f)** Business Associate may create a Limited Data Set and use such Limited Data Set under a Data Use Agreement with Covered Entity that meets the requirements of the Privacy Rule.

**5. OBLIGATIONS OF COVERED ENTITY**

**(a)** Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 C.F.R. § 164.520, to the extent that such limitation may affect

Business Associate's use or disclosure of Protected Health Information.

**(b)** Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

**(c)** Covered Entity shall notify Business Associate of any restriction on the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

**(d)** Covered Entity shall obtain any consent, authorization or permission that may be required by the Privacy Rule or state laws and regulations before disclosing to Business Associate the Protected Health Information pertaining to an Individual.

**6. 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. This provision does not apply to Business Associate's use or disclosure of Protected Health Information for data aggregation or management and administrative activities of Business Associate.

**7. HOLDER OF MASSACHUSETTS PERSONAL INFORMATION**

Business Associate acknowledges that to the extent that Business Associate is a holder of Personal Information as defined by the State Standards (i.e., M.G.L. ch. 93H and the regulations thereunder), Business Associate is subject to and shall have and maintain appropriate security measures to protect Personal Information consistent with provisions of the State Standards. The requisite measures shall include, but not limited to, undertaking requisite responsive actions in the event of a breach of security.

**8. RED FLAGS NOTIFICATION**

To the extent that Business Associate is a Service Provider of Covered Accounts as defined in the Red Flags Rules:

**(a)** Business Associate shall perform its activities under the Agreement in accordance with reasonable policies and procedures Business Associate designed to detect, prevent, and mitigate the risk of identity theft, as required of a Service Provider under the Red Flags Rules (the "Program"); and,

**(b)** Promptly report to Covered Entity any specific incidents which Business Associate detects as to Covered Accounts of Covered Entity pursuant to the Program and, as appropriate under the Agreement, respond to, or reasonably assist Covered Entity in responding to, such reported incidents.

**9. TERM AND TERMINATION**

**(a)** **Term**. The Term of this Addendum shall be effective upon execution, 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 9.

**(b)** **Termination for Cause**. Upon Covered Entity's knowledge of a material breach

of this Addendum 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 Addendum and the Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

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

(3) If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

**(c) Effect of Termination**.

(1) Except as provided in paragraph (2) of this sub-Section (c), upon termination of the Addendum, 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. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

(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 Covered Entity's review and acknowledgement that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Addendum to such Protected Health Information and limit further uses and disclosures of 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.

**10. MISCELLANEOUS**

**(a) Regulatory References**. A reference in this Addendum to a section of the law means the section as in effect or as amended.

**(b) Amendment**. The Parties agree to take such action as is necessary to amend this Addendum from time to time as is necessary for either Party or both Parties to comply with the requirements of the HIPAA Standards, Red Flags Rules or State Standards, as applicable.

**(c) Survival**. The respective rights and obligations of Business Associate under Section 9(c) of this Addendum shall survive the termination of this Addendum. In addition, Sections 2(f) and 2(g) shall survive termination of this Addendum, provided Covered Entity determines that the Protected Health Information being retained under Section 9(c) constitutes a Designated Record Set.

**(d) Interpretation**. Any ambiguity in this Addendum shall be resolved to permit Covered Entity to comply with the HIPAA Standards, Red Flags Rules or State Standards, as applicable.

**(e) Construction of Terms**. The terms of this Addendum shall be construed in light of any applicable interpretation or guidance that may be issued from time to time on the HIPAA Standards by the Department of Health and Human Services or its Office of Civil Rights, or

on the Red Flags Rules or the State Standard by government authorities.

**(f)** **No Third Party Beneficiaries**. Nothing in this Agreement shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

**(g)** **Contradictory Terms**. Any provision of the Agreement that is directly contradictory to one or more terms of this Addendum ("Contradictory Term") shall be superseded by the terms of this Addendum as of the Effective Date of this Addendum to the extent and only to the extent of the contradiction, only for the purpose of the Covered Entity's compliance with the HIPAA Standards, Red Flags Rules or State Standards, and only to the extent that it is reasonably impossible to comply with both the Contradictory Term and the terms of this Addendum.

**(h)** **HITECH Act Applicability**. To the extent not referenced or incorporated herein, requirements applicable to Business Associate and Covered Entity under the HITECH Act are hereby incorporated by reference into this Addendum. Business Associate and Covered Entity agree to comply with applicable requirements imposed under the HITECH Act, as of the effective date of each such requirement.

| **BUSINESS ASSOCIATE** | | **COVERED ENTITY SIGNATURE HEALTHCARE CORPORATION** | |
|---|---|---|---|
| By Signature: | _____ | By Signature: | _____ |
| Print Name: | _____ | Print Name: | _____ |
| Title: | _____ | Title: | _____ |