

## EXHIBIT F

### HIPAA BUSINESS ASSOCIATE AGREEMENT

#### Recitals

- A. This Contract (Agreement) has been determined to or may constitute a business associate relationship under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ('the HITECH Act'), 42 U.S.C. section 17921 et seq., and their implementing privacy and security regulations at 45 CFR Parts 160 and 164 ("the HIPAA regulations").
- B. The Consortium wishes to disclose to Contractor (Business Associate) certain information pursuant to the terms of this Agreement, some of which may constitute Protected Health Information ("PHI"), including protected health information in electronic media ("ePHI"), under federal law, and personal information ("PI") under state law.
- C. As set forth in this Agreement, Contractor, here and after, is or may be the Business Associate of the Consortium and provides services, for the Consortium ("Services") and may create, receive, maintain, transmit, use or disclose PHI and PI thereunder. The Consortium and Business Associate are each a party to this Agreement and are collectively referred to as the "parties."
- D. The purpose of this Addendum is to protect the privacy and security of the PHI and PI that may be created, received, maintained, transmitted, used or disclosed pursuant to this Agreement, and to comply with certain standards and requirements of HIPAA, the HITECH Act and the HIPAA regulations, including, but not limited to, the requirement that the Consortium must enter into a contract containing specific requirements with Contractor prior to the disclosure of PHI to Contractor, as set forth in 45 CFR Parts 160 and 164 and the HITECH Act, and the Final Omnibus Rule as well as the Alcohol and Drug Abuse patient records confidentiality law 42 CFR Part 2, and any other applicable state or federal law or regulation. 42 CFR section 2.1(b)(2)(B) allows for the disclosure of such records to qualified personnel for the purpose of conducting management or financial audits, or program evaluation. 42 CFR Section 2.53(d) provides that patient identifying information disclosed under this section may be disclosed only back to the program from which it was obtained and used only to carry out an audit or evaluation purpose or to investigate or prosecute criminal or other activities, as authorized by an appropriate court order.
- E. The terms used in this Addendum, but not otherwise defined, shall have the same meanings as those terms have in the HIPAA regulations. Any reference to statutory or regulatory language shall be to such language as in effect or as amended.

#### II. Definitions

- A. Breach shall have the meaning given to such term under 45 CFR 164.402 of HIPAA, the HITECH Act, the HIPAA regulations, and the Final Omnibus Rule.
- B. Business Associate shall have the meaning given to such term under 45 CFR 160.103 of HIPAA, the HITECH Act, the HIPAA regulations, and the final Omnibus Rule.
- C. Covered Entity shall have the meaning given to such term under 45 CFR 160.103 of HIPAA, the HITECH Act, the HIPAA regulations, and Final Omnibus Rule.
- D. Electronic Health Record shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C Section 17921 and implementing regulations.
- E. Electronic Protected Health Information (ePHI) means individually identifiable health information transmitted by electronic media or maintained in electronic media, including but not limited to electronic media as set forth under 45 CFR section 160.103.

- F. Individually Identifiable Health Information means health information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer or health care clearinghouse, and relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, that identifies the individual or where there is a reasonable basis to believe the information can be used to identify the individual, as set forth under 45 CFR section 160.103.
- G. Privacy Rule shall mean the HIPAA Regulation that is found at 45 CFR Parts 160 and 164, Subparts A and E.
- H. Personal Information or “PI” shall have the meaning given to such term in California Civil Code section 1798.29, limited to such received from, or received or created pursuant to performance of the Services.
- I. Protected Health Information or “PHI” means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or is transmitted or maintained in any other form or medium, as set forth under 45 CFR section 160.103, limited to such received from, or received or created pursuant to performance of the Services.
- J. Required by law, as set forth under 45 CFR section 164.103, means a mandate contained in law that compels an entity to make a use or disclosure of PHI that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants, subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information, and a civil or an authorized investigative demand. It also includes Medicare conditions of participation with respect to health care providers participating in the program, and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.
- K. Secretary means the Secretary of the U.S. Department of Health and Human Services (“HHS”) or the Secretary's designee.
- L. Security Incident (or “security incident”) means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI or PI, or confidential data that is essential to the ongoing operation of the Business Associate’s organization and intended for internal use; or interference with system operations in an information system.
- M. Security Rule shall mean the HIPAA regulation that is found at 45 CFR Parts 160 and 164, Subparts A and C.
- N. Unsecured PHI shall have the meaning given to such term under the HITECH Act, 42 U.S.C. section 17932(h), any relevant guidance issued pursuant to such Act, and the HIPAA regulations.

### **III. Terms of Agreement**

#### **A. Permitted Uses and Disclosures of PHI by Business Associate**

***Permitted Uses and Disclosures.*** Except as otherwise indicated in this Addendum, Business Associate may use or disclose PHI only to perform functions, activities or services specified in this Agreement, for, or on behalf of the Consortium, provided that such use or disclosure would not violate the Privacy Rule, if done by the Consortium. Any such use or disclosure must, to the extent practicable, be limited to the limited data set, as defined in 45 CFR section 164.514(e)(2), or, if needed, to the minimum necessary to accomplish the intended purpose of such use or disclosure, in compliance with the HITECH Act and

any guidance issued pursuant to such Act, the HIPAA regulations, the Final Omnibus Rule and 42 CFR Part 2, if applicable.

1. ***Specific Use and Disclosure Provisions.*** Except as otherwise indicated in this Addendum, Business Associate may:

- a. ***Use and disclose for management and administration.*** Use and disclose PHI for the proper management and administration of the Business Associate provided that such disclosures are required by law, or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and will be 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 that the confidentiality of the information has been breached.
- b. ***Provision of Data Aggregation Services.*** Use PHI to provide data aggregation services to the Consortium. Data aggregation means the combining of PHI created or received by the Business Associate on behalf of the Consortium with PHI received by the Business Associate in its capacity as the Business Associate of another covered entity, to permit data analyses that relate to the health care operations of the Consortium.

## **B. Prohibited Uses and Disclosures**

1. Business Associate shall not disclose PHI about an individual to a health plan for payment or health care operations purposes if the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full and the individual requests such restriction, in accordance with 42 U.S.C. section 17935(a) and 45 CFR section 164.522(a).
2. Business Associate shall not directly or indirectly receive remuneration in exchange for PHI, except with the prior written consent of the Consortium and as permitted by 42 U.S.C. section 17935(d)(2).

## **C. Responsibilities of Business Associate**

Business Associate agrees:

1. ***Nondisclosure.*** Not to use or disclose Protected Health Information (PHI) other than as permitted or required by this Agreement or as required by law.
2. ***Safeguards.*** To implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic PHI, that it creates, receives, maintains, uses or transmits on behalf of the Consortium, in compliance with 45 CFR sections 164.308, 164.310 and 164.312, and to prevent use or disclosure of PHI other than as provided for by this Agreement. Business Associate shall implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of 45 CFR section 164, subpart C, in compliance with 45 CFR section 164.316. Business Associate shall develop and maintain a written information security and awareness training program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Business Associate's operations and the nature and scope of its activities, and which incorporates the requirements of section 3, Security, below, as required under 45 CFR 164.308.
3. ***Security.*** To take reasonable steps designed to ensure the continuous security of all of its computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:
  - a. Complying with all of the data system security precautions listed in Attachment A, the Business Associate Data Security Requirements;
  - b. Achieving and maintaining compliance with the HIPAA Security Rule (45 CFR Parts 160 and 164) with respect to ePHI, as necessary in performing Services for the Consortium under this Agreement;
  - c. Intentionally Omitted.
  - d. In case of a conflict between any of the security standards contained in any of these enumerated sources of security standards, the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to PHI from unauthorized disclosure.

Further, Business Associate must comply with changes to these standards that occur after the effective date of this Agreement.

Business Associate has designated a security official who is responsible for developing and implementing its security policies and procedures as required in 45 CFR 164.308. Business Associate shall also designate an appropriate individual for communicating on security matters relating to the requirements of this section with the Consortium. Except as otherwise expressly agreed in the Agreement, nothing shall require Business Associate to be responsible for the implementation and maintenance of any controls concerning the equipment or information systems of Consortium; as such controls shall be the responsibility of Consortium.

**D. *Mitigation of Harmful Effects.*** To mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate or its subcontractors in violation of the requirements of this Addendum.

**E. *Business Associate's Agents and Subcontractors.***

1. To enter into written agreements with any agents, including subcontractors and vendors, to whom Business Associate provides PHI or PI received from or created or received by Business Associate on behalf of the Consortium, that impose the same restrictions and conditions on such agents, subcontractors and vendors that apply to Business Associate with respect to such PHI and PI under this Addendum, and that comply with all applicable provisions of HIPAA, the HITECH Act the HIPAA regulations, and the Final Omnibus Rule, including the requirement that any agents, subcontractors or vendors implement reasonable and appropriate administrative, physical, and technical safeguards to protect such PHI and PI. Business associates may be directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by its contract or required by law. A business associate also may be directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule. A "business associate" also is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate. Business Associate shall incorporate, when applicable, the relevant provisions of this Addendum into each subcontract or subaward to such agents, subcontractors and vendors, including the requirement that any security incidents affecting ePHI or breaches of unsecured PHI or PI be reported to Business Associate.
2. In accordance with 45 CFR section 164.504(e)(1)(ii), upon Business Associate's knowledge of a material breach or violation by its subcontractor of the agreement between Business Associate and the subcontractor, Business Associate shall:
  - a. Provide written notice and an opportunity for the subcontractor to cure the breach or end the violation and may terminate the agreement if the subcontractor does not cure the breach or end the violation within the time specified by Business Associate, which shall in no event be longer than three (3) business days; or
  - b. If feasible, immediately terminate the agreement if the subcontractor has breached a material term of the agreement and cure is not possible.

**F. *Availability of Information to DHCS and Individuals.*** To provide access and information:

1. To provide access as the Consortium may require, and in the time and manner designated by the Consortium (upon reasonable notice and during Business Associate's normal business hours) to PHI maintained by Business Associate in a Designated Record Set, to the Consortium in accordance with 45 CFR section 164.524. Designated Record Set means the group of records maintained for the Consortium that includes medical, dental and billing records about individuals; enrollment, payment, claims adjudication, and case or medical management systems maintained for the Consortium health plans; or those records used to make decisions about individuals on behalf of the Consortium. Business Associate shall use the forms and processes developed by the Consortium and provided to Business Associate in writing advance for this purpose and shall respond to requests for access to

records transmitted by the Consortium within fifteen (15) calendar days of receipt of the request by producing the records or verifying that there are none.

2. If Business Associate maintains an Electronic Health Record with PHI, and an individual requests a copy of such information in an electronic format, Business Associate shall provide such information in an electronic format to enable the Consortium to fulfill its obligations under the HITECH Act, including but not limited to, 42 U.S.C. section 17935(e).
3. If Business Associate receives data from the Consortium that was provided to the Consortium by the Social Security Administration and identified as such, upon request by the Consortium, Business Associate shall provide the Consortium with a list of all employees, contractors and agents who have access to the Social Security data, including employees, contractors and agents of its subcontractors and agents.

**G. Amendment of PHI.** To make any amendment(s) to PHI that the Consortium directs or agrees to pursuant to 45 CFR section 164.526, in the reasonable time and manner designated by the Consortium.

**H. Internal Practices.** To make Business Associate's internal practices, books and records relating to the use and disclosure of PHI received from the Consortium, or created or received by Business Associate on behalf of the Consortium, available to the Secretary of the U.S. Department of Health and Human Services in a time and manner designated by the Secretary, for purposes of determining the Consortium's compliance with the HIPAA regulations. If any information needed for this purpose is in the exclusive possession of any other entity or person, Business Associate shall make reasonable efforts to obtain the information.

**I. Documentation of Disclosures.** To document and make available to the Consortium such disclosures of PHI, and information related to such disclosures, necessary to respond to a proper request by the subject Individual for an accounting of disclosures of PHI, in accordance with the HITECH Act and its implementing regulations, including but not limited to 45 CFR section 164.528 and 42 U.S.C. section 17935(c). If Business Associate maintains electronic health records for the Consortium as of January 1, 2009, Business Associate must provide an accounting of disclosures, including those disclosures for treatment, payment or health care operations, effective with disclosures on or after January 1, 2014. If Business Associate acquires electronic health records for the Consortium after January 1, 2009, Business Associate must provide an accounting of disclosures, including those disclosures for treatment, payment or health care operations, effective with disclosures on or after the date the electronic health record is acquired, or on or after January 1, 2011, whichever date is later. The electronic accounting of disclosures shall be for disclosures during the three years prior to the request for an accounting.

**J. Breaches and Security Incidents.** During the term of this Agreement, Business Associate agrees to implement reasonable procedures and practices for the discovery and prompt reporting of any breach of unsecured PHI or security incident, and to take the following steps:

1. **Notice to the Consortium.** (1) To notify the Consortium **immediately** upon, and no later than 48 hours from, the discovery of a security incident that involves unauthorized use or disclosure of data provided to the Consortium by the Social Security Administration; provided that, such data was identified as such when provided to Business Associate. This notification will be **by telephone call plus email or fax** upon the discovery of the breach. (2) To notify the Consortium **within 48 hours by email or fax** of the discovery of unsecured PHI or PI in electronic media or in any other media if the PHI or PI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, any security incident affecting ePHI, or unauthorized access, use or disclosure of PHI or PI by Business Associate in violation of this Agreement and this Addendum. A breach shall be treated as discovered by Business Associate as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of Business Associate. Notice shall be provided to the Consortium Program Contract Manager, the Consortium Privacy Officer and the Consortium Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves data provided to the Consortium by the Social Security

Administration, notice shall be provided by calling the Consortium's Service Desk. Notice shall be given to the Consortium Executive Director, including all information known at the time, via email. Upon discovery of such a breach or security incident, or unauthorized access, use or disclosure of PHI or PI, Business Associate shall take:

- a. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and
  - b. Any action pertaining to such unauthorized disclosure required by Federal and State laws and regulations applicable to Business Associate.
2. ***Investigation and Investigation Report.*** To immediately investigate such security incident, breach, or unauthorized access, use or disclosure of PHI or PI. If the initial report did not include all of the requested information marked with an asterisk, then within 72 hours of the discovery, Business Associate shall submit an updated form containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the Consortium Program Contract Manager, the Consortium Privacy Officer, and the Consortium Information Security Officer:
  3. ***Security Incident Report.*** To provide a report of the investigation to the Consortium Executive Director and the Consortium Information Security Officer within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. If all of the required information was not included in either the initial report, or the Investigation Report, then a separate Security Incident Report must be submitted. The report shall be submitted on the approved Security Incident Report form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable provisions of HIPAA, the HITECH Act, the HIPAA regulations and/or state law. The report shall also include a corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If the Consortium requests information in addition to that listed on the designated form, Business Associate shall make reasonable efforts to provide the Consortium with such information. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated form. The Consortium will review and approve or disapprove, in collaboration with Business Associate, the determination of whether a breach occurred, is reportable to the appropriate entities, and if individual notifications are required.
  4. ***Notification of Individuals.*** To the extent that a breach of PHI or PI is caused by Business Associate's or its subcontractors', agents' or vendors' breach of this Addendum, Business Associate shall reimburse the Consortium for any reasonable and direct out-of-pocket costs of such legally required notifications to affected individuals associated with the breach. The notifications shall comply with the requirements set forth in 42 U.S.C. section 17932 and its implementing regulations, including, but not limited to, the requirement that the notifications be made without unreasonable delay and in no event later than 60 calendar days. The Consortium Program Contract Manager, the Consortium Privacy Officer, and the Consortium Information Security Officer shall approve the time, manner and content of and send any such notifications and their review and approval must be obtained before the notifications are made.
  5. ***Responsibility for Reporting of Breaches.*** If the cause of a breach of PHI or PI is attributable to Business Associate or its agents, subcontractors or vendors, Business Associate is responsible for providing to the Consortium all required reporting information of the breach as specified in 42 U.S.C. section 17932 and its implementing regulations, including notification to media outlets and to the Secretary. If a breach of unsecured PHI involves more than 500 residents of the State of California or its jurisdiction, Business Associate shall provide information to the Consortium required to notify the Secretary of the breach immediately upon discovery of the breach. If Business Associate has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to the Consortium in

addition to Business Associate, Business Associate shall notify the Consortium, and the Consortium and Business Associate may take appropriate action to prevent duplicate reporting. The breach reporting requirements of this paragraph are in addition to the reporting requirements set forth in subsection 1, above.

6. ***The Consortium Contact Information.*** To direct communications to the above referenced Consortium staff, the Contractor shall initiate contact as indicated herein. The Consortium reserves the right to make changes to the contact information below by giving written notice to the Contractor. Said changes shall not require an amendment to this Addendum or the Agreement to which it is incorporated.

The Consortium <b>John Boule, Executive Director</b>
Contractor: Rachel Frey, Principal

**K. *Termination of Agreement.*** In accordance with Section 13404(b) of the HITECH Act and to the extent required by the HIPAA regulations, if Business Associate knows of a material breach or violation by the Consortium of this Addendum, it shall take the following steps:

1. Provide an opportunity for the Consortium to cure the breach or end the violation and terminate the Agreement if the Consortium does not cure the breach or end the violation within the time specified by Business Associate; or
2. Immediately terminate the Agreement if the Consortium has breached a material term of the Addendum and cure is not possible.

**L. *Due Diligence.*** Business Associate shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this Addendum and is in compliance with applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations, and that its agents, subcontractors and vendors are in compliance with their obligations as required by this Addendum.

**M. *Sanctions and/or Penalties.*** Business Associate understands that a failure to comply with the provisions of HIPAA, the HITECH Act and the HIPAA regulations that are applicable to Business Associate may result in the imposition of sanctions and/or penalties on Business Associate under HIPAA, the HITECH Act and the HIPAA regulations.

#### **IV. Obligations of the Consortium**

The Consortium agrees to:

- A. *Permission by Individuals for Use and Disclosure of PHI.*** Provide the Business Associate with any changes in, or revocation of, permission by an Individual to use or disclose PHI, if such changes affect the Business Associate's permitted or required uses and disclosures.
- B. *Notification of Restrictions.*** Notify the Business Associate of any restriction to the use or disclosure of PHI that the Consortium has agreed to in accordance with 45 CFR section 164.522, to the extent that such restriction may affect the Business Associate's use or disclosure of PHI.
- C. *Requests Conflicting with Law.*** Not request the Business Associate to use or disclose PHI or PI in any manner that would not be permissible under the HIPAA regulations or any other applicable law if done by the Consortium.
- D. *Disclosures Conflicting with Law.*** Not disclose PHI or PI to Business Associate in violation of the HIPAA regulations or any other applicable law.

#### **V. Audits, Inspection and Enforcement**

- A.** From time to time, the Consortium may request information from Business Associate to monitor compliance with this Addendum no more than once per calendar year during the term of this Addendum. Business Associate shall promptly respond to a written information security questionnaire provided by the Consortium that pertains to Business Associate's administrative, technical and physical security controls relevant to Business Associate's safeguards for PHI or PI or to make appropriate personnel reasonably available by telephone to provide such information verbally. The Consortium shall not

disclose such proprietary questionnaire responses or information provided by Business Associate in connection therewith, or refer to or release such questionnaire or information in any communication to any person or entity other than the Consortium, unless required by law or with Business Associate's written consent. The fact that the Consortium requests, or fails to request, or has the right to request such information, does not relieve Business Associate of its responsibility to comply with this Addendum, nor does the Consortium's:

1. Failure to detect or
  2. Detection, but failure to notify Business Associate or request Business Associate's remediation of any unsatisfactory practices constitute acceptance of such practice or a waiver of the Consortium's enforcement rights under this Agreement and this Addendum.
- B.** If Business Associate is the subject of an audit, compliance review, or complaint investigation by the Secretary or the Office of Civil Rights, U.S. Department of Health and Human Services, that is related to the performance of its obligations pursuant to this HIPAA Business Associate Addendum, Business Associate shall, to the extent permitted by law, notify the Consortium and provide the Consortium with a copy of any PHI or PI that Business Associate provides to the Secretary or the Office of Civil Rights concurrently with providing such PHI or PI to the Secretary. As between the parties, Business Associate, not CONSORTIUM, is responsible for any civil penalties assessed against Business Associate due to any such audit or investigation of Business Associate, in accordance with 42 U.S.C. section 17934(c).

## **VI. Termination**

- A. *Term.*** The Term of this Addendum shall commence as of the effective date of this Addendum and shall extend beyond the termination of the contract and shall terminate when all the PHI provided by the Consortium to Business Associate, or created or received by Business Associate on behalf of the Consortium, is destroyed or returned to the Consortium, in accordance with 45 CFR 164.504(e)(2)(ii)(I).
- B. *Termination for Cause.*** In accordance with 45 CFR section 164.504(e)(1)(ii), upon the Consortium's knowledge of a material breach or violation of this Addendum by Business Associate, the Consortium shall:
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 the Consortium; or
  2. Immediately terminate this Agreement if Business Associate has breached a material term of this Addendum and cure is not possible.
- C. *Judicial or Administrative Proceedings.*** Business Associate will, to the extent permitted by law, notify the Consortium if it is named as a defendant in a criminal proceeding for a violation of HIPAA. The Consortium may terminate this Agreement if Business Associate is found guilty of a criminal violation of HIPAA. The Consortium may terminate this Agreement if a finding or stipulation that the Business Associate has violated any material standard or requirement of HIPAA, or other security or privacy laws governing PHI or PI is made in any administrative or civil proceeding in which the Business Associate is a party or has been joined.
- D. *Effect of Termination.*** Upon termination or expiration of this Agreement for any reason, Business Associate shall return or destroy all PHI received from the Consortium (or created or received by Business Associate on behalf of the Consortium) that Business Associate still maintains in any form, and shall retain no copies of such PHI. If return or destruction is not feasible, Business Associate shall notify the Consortium of the conditions that make the return or destruction infeasible, and the Consortium and Business Associate shall determine the terms and conditions under which Business Associate may retain the PHI. Business Associate shall continue to extend the protections of this Addendum to such PHI, and shall limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate.



## VII. Miscellaneous Provisions

- A. *Disclaimer.*** The Consortium makes no warranty or representation that compliance by Business Associate with this Addendum, HIPAA or the HIPAA regulations will be adequate or satisfactory for Business Associate's own purposes or that any information in Business Associate's possession or control, or transmitted or received by Business Associate, is or will be secure from unauthorized use or disclosure. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI.
- B. *Amendment.*** The parties acknowledge that federal and state laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Addendum may be required to provide for procedures to ensure compliance with any changes in such laws. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, the HIPAA regulations and other applicable laws relating to the security or privacy of PHI. Upon the Consortium's request, Business Associate agrees to promptly enter into negotiations with the Consortium concerning an amendment to this Addendum embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, the HIPAA regulations or other applicable laws. The Consortium may terminate this Agreement for convenience upon thirty (30) days written notice in the event:
1. Business Associate does not promptly enter into negotiations to amend this Addendum when requested by the Consortium pursuant to this Section; or
  2. Business Associate does not enter into an amendment providing assurances regarding the safeguarding of PHI that the Consortium in its sole discretion, deems sufficient to satisfy the standards and requirements of HIPAA and the HIPAA regulations.
- C. *Assistance in Litigation or Administrative Proceedings.*** Business Associate shall reasonably cooperate with the Consortium in the event of litigation or administrative proceedings being commenced against the Consortium, its directors, officers or employees based upon claimed violation of HIPAA, the HIPAA regulations or other laws relating to security and privacy of PHI or PI by the Business Associate, except where Business Associate or its subcontractor, employee or agent is a named party.
- D. *No Third-Party Beneficiaries.*** Nothing express or implied in the terms and conditions of this Addendum is intended to confer, nor shall anything herein confer, upon any person other than the Consortium or Business Associate and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.
- E. *Interpretation.*** The terms and conditions in this Addendum shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, the HIPAA regulations and applicable state laws. The parties agree that any ambiguity in the terms and conditions of this Addendum shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act and the HIPAA regulations.
- F. *Regulatory References.*** A reference in the terms and conditions of this Addendum to a section in the HIPAA regulations means the section as in effect or as amended.
- G. *Survival.*** The respective rights and obligations of Business Associate under Section VI.D of this Addendum shall survive the termination or expiration of this Agreement.
- H. *No Waiver of Obligations.*** No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.

## Attachment A

### Business Associate Data Security Requirements

#### I. Personnel Controls

- A. *Employee Training.*** All workforce members who assist in the performance of the Services on behalf of the Consortium, or access or disclose the Consortium PHI or PI must complete information privacy and security training, at least annually, at Business Associate's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following contract termination.
- B. *Employee Discipline.*** Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.
- C. *Confidentiality Statement.*** All persons that will be working with the Consortium PHI or PI must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to the Consortium PHI or PI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for the Consortium inspection for a period of six (6) years following contract termination.
- D. *Background Check.*** Before a member of the workforce may access the Consortium PHI or PI, a thorough background check of that worker must be conducted, with evaluation of the results to assure that there is no indication that the worker may present a risk to the security or integrity of confidential data or a risk for theft or misuse of confidential data. The Contractor shall retain each workforce member's background check documentation for a period of three (3) years following contract termination.

#### II. Technical Security Controls

- A. *Workstation/Laptop encryption.*** All workstations and laptops that process and/or store the Consortium PHI or PI must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the Consortium Information Security Office.
- B. *Server Security.*** Servers containing unencrypted the Consortium PHI or PI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.
- C. *Minimum Necessary.*** Only the minimum necessary amount of the Consortium PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.
- D. *Removable media devices.*** All electronic files that contain the Consortium PHI or PI data must be encrypted when stored on any removable media or portable device (i.e. flash drives, CD/DVD, smartphones, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.
- E. *Antivirus software.*** All workstations, laptops and other systems that process and/or store the Consortium PHI or PI must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

- F. *Patch Management.*** All workstations, laptops and other systems that process and/or store the Consortium PHI or PI must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release.
- G. *User IDs and Password Controls.*** All users must be issued a unique user name for accessing the Consortium PHI or PI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within one (1) business day. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every 90 days, preferably every 60 days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:
- Upper case letters (A-Z)
  - Lower case letters (a-z)
  - Arabic numerals (0-9)
  - Non-alphanumeric characters (punctuation symbols)
- H. *Data Destruction.*** When no longer needed, all the Consortium PHI or PI must be deleted and prior to disposal of hardware, all the Consortium PHI or PI must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the PHI or PI cannot be retrieved.
- I. *System Timeout.*** The system providing access to the Consortium PHI or PI must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.
- J. *Warning Banners.*** All systems providing access to the Consortium PHI or PI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.
- K. *System Logging.*** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for the Consortium PHI or PI, or which alters the Consortium PHI or PI. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If the Consortium PHI or PI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least one (1) year after occurrence.
- L. *Access Controls.*** The system providing access to the Consortium PHI or PI must use role based access controls for all user authentications, enforcing the principle of least privilege.
- M. *Transmission encryption.*** All data transmissions of the Consortium PHI or PI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing PHI can be encrypted. This requirement pertains to any type of PHI or PI in motion such as website access, file transfer, and E-Mail.

- N. **Intrusion Detection.** All systems involved in accessing, holding, transporting, and protecting the Consortium PHI or PI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

### III. Audit Controls

- A. **System Security Review.** All systems processing and/or storing the Consortium PHI or PI must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.
- B. **Log Reviews.** All systems processing and/or storing the Consortium PHI or PI must have a routine procedure in place to review system logs for unauthorized access.
- C. **Change Control.** All systems processing and/or storing the Consortium PHI or PI must have a documented change control procedure designed to ensure separation of duties and protect the confidentiality, integrity and availability of data.

### IV. Business Continuity / Disaster Recovery Controls

- A. **Emergency Mode Operation Plan.** Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic the Consortium PHI or PI in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than 24 hours.
- B. **Data Backup Plan.** Contractor must have established documented procedures to backup confidential information on Contractor systems. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore the confidential information should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of the confidential information .

### V. Paper Document Controls

- A. **Supervision of Data.** The Consortium PHI or PI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. The Consortium PHI or PI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.
- B. **Escorting Visitors.** Visitors to areas where the Consortium PHI or PI in paper form is contained shall be escorted and such Consortium PHI or PI shall be kept out of sight while visitors are in the area.
- C. **Confidential Destruction.** The Consortium PHI or PI in paper form must be disposed of through confidential means, such as cross cut shredding and pulverizing.
- D. **Removal of Data.** The Consortium PHI or PI in paper form must not be removed from the permitted locations where the Contractor is permitted to perform the Services except with express written permission of the Consortium.
- E. **Faxing.** Faxes containing the Consortium PHI or PI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.

- F. *Mailing.*** Mailings of the Consortium PHI or PI in paper form shall be sealed and secured from damage or inappropriate viewing of PHI or PI to the extent possible. Mailings which include 500 or more individually identifiable records of the Consortium PHI or PI in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of the Consortium to use another method is obtained.