

## BUSINESS ASSOCIATE AGREEMENT

This Business Associate Addendum supplements and is made a part of the California Children's Services Memorandum of Understanding ("MOU") is by and between the County of Monterey, a political subdivision of the State of California, on behalf of the Monterey County Health Department ("**Business Associate**") and Santa Cruz-Monterey-Merced Managed Medical Care Commission, a California public entity, doing business as Central California Alliance for Health ("**Covered Entity**"). This Agreement is effective as of the date of the MOU.

Business Associate s certain services for Covered Entity MOU that involve the use or disclosure of **Protected Health Information** (as defined in section I.E) that is created, received, transmitted, used, disclosed, or maintained by Business Associate on or behalf of Covered Entity.

The parties are committed to complying with the requirements of the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (that act, the "**HITECH Act**"), the final regulations to such Acts that the U.S. Department of Health and Human Services has promulgated and stated in 45 C.F.R. Parts 160, 162, and 164 (collectively, the "**HIPAA Rules**"), and subject to any necessary approval and required changes by the Department of Health Care Services ("**DHCS**").

The parties therefore agree as follows:

### I. Definitions.

- A. "**Breach**" has the meaning given that term in 45 C.F.R. section 164.402.
- B. "**Discovery**" means the first day on which an Incident (as defined in section II.F) is known to Business Associate (including any person that is an employee, officer, or **Subcontractor** of Business Associate), or should reasonably have been known to Business Associate, to have occurred.
- C. "**Electronic Health Record**" has the meaning given that term in the HITECH Act, including, but not limited to, 42 U.S.C section 17921 and implementing regulations.
- D. "**Individual**" has the meaning given that term in 45 C.F.R. section 160.103 and includes a person who qualifies as a personal representative in accordance with 45 C.F.R. section 164.502(g).
- E. "**Protected Health Information**" has the meaning given that term in 45 C.F.R. section 160.103, limited to the information created, received, transmitted, or maintained by Business Associate on behalf of or for Covered Entity. In this agreement Protected Health Information ("**PHI**") includes **Electronic Protected Health Information** as defined in 45 C.F.R. section 160.103.
- F. "**Secretary**" means the Secretary of the U.S. Department of Health and Human Services or his or her designee.
- G. "**Security Incident**" has the meaning given that term in 45 C.F.R. section 164.304.
- H. Terms used but not otherwise defined in this agreement have the meanings given those terms in the HIPAA Rules. A regulatory reference in this agreement means the section as in effect or as amended for which compliance is required.

## II. Business Associate's Obligations.

A. **Permitted Use and Disclosure of PHI.** Business Associate shall use and disclose PHI only as permitted by this agreement, or as **Required By Law** (as defined in 45 C.F.R. section 164.103), provided that Business Associate shall not use or disclose PHI in any manner that would constitute a violation of the HIPAA Rules if done by Covered Entity. Business Associate is only permitted to:

1. Use or disclose PHI to perform its obligations and functions under the MOU;
2. Use PHI for the proper management and administration of Business Associate or to carry out its legal responsibilities;
3. Disclose PHI for the proper management and administration of Business Associate or to carry out its legal responsibilities, if such disclosure is Required By Law, or if Business Associate obtains (i) reasonable assurances from the recipient that the recipient will keep the PHI confidential, and will use or further disclose the PHI only as Required By Law or for the purpose for which it was disclosed to the recipient, and (ii) a written agreement from such third party to immediately notify Business Associate of any instance of which the recipient is aware in which the confidentiality of the PHI has been breached;
4. Use PHI to provide **Data Aggregation** services (as defined in 45 C.F.R. section 164.501) to Covered Entity as permitted by 45 C.F.R. section 164.504(e)(2)(i)(B) to the extent specified in the MOU;
5. Use or disclose PHI to report violations of the law to law enforcement or as otherwise Required By Law; and
6. Use PHI obtained by Business Associate under MOU to create de-identified information consistent with the standards of 45 C.F.R. section 164.514.

B. **Safeguards.** Business Associate shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI that Business Associate creates, receives, maintains, uses, discloses, or transmits on behalf of Covered Entity, as required by the HIPAA Rules. Business Associate shall comply with the requirements in 45 C.F.R. Part 164, subpart C as well as the provisions stated in Appendix A. Business Associate shall document policies and procedures that implement such safeguards and shall provide them to Covered Entity upon request (who may further disclose them as required by DHCS).

C. **Minimum Necessary.** Business Associate and its agents and Subcontractors shall request, use and disclose only the minimum necessary amount of PHI necessary to accomplish the purpose of the request, use or disclosure (as described in 45 C.F.R. section 164.502(b) and section 164.514(d)). To the extent practicable, all uses and disclosures must be restricted to information in a limited data set (as described in 45 C.F.R. section 164.514(e)(2)).

D. **Prohibited Uses and Disclosures.** Business Associate shall not use or disclose PHI for any purpose other than as specifically permitted by this agreement. Specifically, but without limitation, Business Associate (a) shall not use or disclose PHI for fundraising or marketing purposes, (b) shall not disclose PHI to a health plan for payment or health care operations purposes if the patient has requested a special restriction on disclosure and has paid out of pocket in full for the health care item or services to

which the PHI solely relates, and (c) shall not directly or indirectly receive remuneration in exchange for PHI (except if submission of PHI to Covered Entity is necessary for Covered Entity to pay Business Associate for performing services for Covered Entity, or with Covered Entity's consent and as permitted by 42 U.S.C. section 17935(d)(2)).

E. **Agents and Subcontractors.** Business Associate agrees to ensure that any agent or Subcontractor to whom it provides PHI agrees in writing to the same restrictions and conditions that apply through this agreement to Business Associate.

F. **Incident Reporting, Mitigation, and Remediation.** Business Associate shall report to Covered Entity any of the following without unreasonable delay but in no event later than within 24 hours after Discovery of such event by Business Associate or any Subcontractor: (i) any acquisition, access, use or disclosure of PHI not provided for in this agreement or the MOU; (ii) any Security Incident involving PHI; (iii) any Breach of Unsecured PHI; and (iv) any loss, destruction, alteration, or other event in which PHI cannot be accounted for (collectively, an "Incident"). Business Associate shall implement reasonable systems for the Discovery and prompt reporting of any Incidents.

1. **Reporting Requirements.** Business Associate shall report the information described below to Covered Entity within 24 hours following Discovery of an Incident, except when despite all reasonable efforts by Business Associate to obtain the information required, circumstances beyond the control of Business Associate necessitate additional time. Under such circumstances, Business Associate shall notify Covered Entity within 24 hours that the Incident has occurred and provide the information required below as soon as possible and without unreasonable delay, but in no event later than within five days from the date of Discovery of the Incident. In the event that Covered Entity requires that Business Associate provide such notice, the notice shall be in the form and format requested by Covered Entity and shall include:

- i. the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, disclosed, lost, altered, destroyed, or otherwise unaccounted for;
- ii. the date of the Incident;
- iii. the date of the Discovery of the Incident;
- iv. a description of the types of PHI that were involved; and
- v. any other details reasonably requested by Covered Entity.

2. **Risk Assessment.** In the event of an Incident, Business Associate shall assist Covered Entity in performing (or at Covered Entity's direction, perform) a risk assessment to determine if there is a low probability that the PHI has been compromised. To enable Covered Entity to make a determination whether or not there is a low probability that PHI has been compromised, Business Associate, and any Subcontractor of Business Associate, shall promptly undertake a risk assessment that addresses the following factors and provide the results of such risk assessment to Covered Entity:

- i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

- ii. the unauthorized person who used the PHI or to whom the disclosure was made;
  - iii. whether the PHI was actually acquired or viewed; and
  - iv. the extent to which the risk to the PHI has been mitigated.
- 3. **Breach Determination and Notification.** Covered Entity shall make the ultimate determination, in its sole discretion, whether there has been a Breach and if so, whether the required notifications, including to Individuals, third parties, the media, and regulators (such as the Secretary and state regulators), will be provided by Covered Entity or Business Associate. In the event that Covered Entity requires that Business Associate provide such notifications regarding a Breach, any such notices must be approved, in advance, by Covered Entity. Covered Entity's approval shall also be required for the manner of delivering notice of a Breach.
- 4. **Record Requirements.** Business Associate shall maintain complete records regarding any Incident for the period required by 45 C.F.R. section 164.530(j) or such longer period Required By Law, and shall make such records available to Covered Entity promptly upon request, but in no event later than within five business days.
- 5. **Costs and Expenses.** Business Associate shall be responsible for all costs and expenses incurred in connection with any Incident, including all costs and expenses stated in section II.L.
- 6. **Mitigation and Remediation.** Business Associate shall mitigate, to the extent practicable and at its cost, any harmful effects from any Incident (including steps to protect the operating environment). Business Associate also shall take prompt steps designed to prevent the recurrence of any Incident. All such efforts shall be subject to the Covered Entity's prior written approval. Business Associate must document a corrective action plan, including information on measures that were taken to halt and/or contain the Incident, and provide such documentation to Covered Entity immediately upon request. Business Associate must comply with this provision regardless of any actions taken by Covered Entity.
- 7. **Ongoing Assistance.** Business Associate shall make itself and any employees, Subcontractors, or agents assisting Business Associate in the performance of its obligations available to Covered Entity at no cost to Covered Entity to testify as witnesses, or otherwise, in the event of an Incident that results in litigation or administrative proceedings against Covered Entity, its directors, officers, agents or employees, or against the DHCS, based upon a claimed violation of laws relating to security and privacy or arising out of this agreement.
- 8. **Unsuccessful Security Incidents.** Notwithstanding the foregoing, Business Associate shall not be required to report to Covered Entity the occurrence of an unsuccessful Security Incident; however Business Associate shall provide to Covered Entity a report of unsuccessful Security Incidents upon reasonable request. In this agreement, an unsuccessful Security Incident shall include, without limitation, activity such as pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denial of service,

and any combination of the above, so long as such activity does not result in unauthorized access, use, acquisition, or disclosure of PHI.

G. **Identification of Employees.** Business Associate shall maintain a current list of its employees, agents, and Subcontractors with access to PHI provided by Covered Entity. Upon request, Business Associate shall provide such list to Covered Entity within a reasonable amount of time.

H. **Access to PHI.** To the extent that Business Associate possesses PHI in a **Designated Record Set** (as defined in 45 C.F.R. section 164.501), and within a reasonable amount of time (but not to exceed ten days) of receipt of a written request from Covered Entity to access such PHI, Business Associate shall transmit such information to Covered Entity. If an Individual requests access to PHI directly from Business Associate, Business Associate will forward such a request in writing to Covered Entity within a reasonable amount of time (but not to exceed ten days). Covered Entity will be responsible for making all determinations regarding the granting or denial of an Individual's request, and Business Associate shall make no such determinations. If Business Associate maintains PHI in electronic format, Business Associate shall provide such information in electronic format to Covered Entity if requested. 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 Covered Entity to fulfill its obligations under the HITECH Act, including but not limited to, 42 U.S.C. section 17935(e).

I. **Amendment of PHI.** Business Associate agrees to make any amendment(s) to PHI that Covered Entity directs or agrees to, in accordance with 45 C.F.R. section 164.526, in the time and manner designated by Covered Entity. Within a reasonable amount of time of receipt of a request by an Individual to Business Associate to amend PHI (but not to exceed five days), Business Associate shall forward to Covered Entity any such requests in writing. Covered Entity shall be responsible for making all determinations regarding amendments to PHI, and Business Associate shall make no such determinations.

J. **Accounting.** Business Associate shall document such disclosures of PHI as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. section 164.528. If Business Associate maintains or acquires Electronic Health Records for Covered Entity, Business Associate must also document disclosures for treatment, payment, or health care operations and provide an accounting of such disclosures upon request. Business Associate agrees to implement a process that allows for an accounting to be collected and maintained by Business Associate and its agents or Subcontractors for at least 6 years prior to the request (except with respect to Electronic Health Records, for which an accounting need only be provided for 3 years prior to the request). In addition, Business Associate agrees that:

1. Within a reasonable amount of time of receipt of a written notice from Covered Entity requesting an accounting of PHI disclosures (but not to exceed ten (10) days), Business Associate shall provide Covered Entity with records of such disclosures containing the information outlined in 45 C.F.R. section 164.528(b). This requirement will apply equally to disclosures for treatment, payment, or health care operations involving Electronic Health Records.
2. Within a reasonable amount of time of receipt of a request by an Individual to Business Associate for an accounting of disclosures of PHI (but not to exceed ten (10) days), Business Associate shall forward to Covered Entity any such requests in writing. Covered Entity shall be responsible for providing an accounting of PHI

disclosures to the Individual. Business Associate will not provide an accounting of its disclosures directly to the Individual.

K. **Government Access.** Upon request, Business Associate shall make its internal practices, books and records relating to the use and disclosure of PHI available to regulatory bodies and to the Secretary to the extent required for determining Covered Entity's compliance with the HIPAA Rules. Business Associate shall concurrently provide Covered Entity with a copy of any PHI that Business Associate provides in accordance with any governmental inquiry.

L. **Indemnification.** Business Associate, at its own expense, agrees to defend, indemnify and hold harmless Covered Entity and any of Covered Entity's affiliates, subsidiaries, directors, officers, employees, representatives and agents from and against any claim, demand, cause of action, class action, cross-claim, arbitration, judgment, liability, damage, fines, penalties, public relations expenses, government investigation or inquiry, remediation and mitigation efforts (including but not limited to notification letters, credit monitoring services, identity theft insurance, reimbursement for credit freezes, fraud resolution services, identity restoration services, toll free information services for affected Individuals, and any similar service that entities make available to impacted Individuals in the event of an Incident), and costs and expenses relating thereto (including but not limited to costs of defense, settlement, adjudication, dismissal, expert fees, court costs, investigation expenses, discovery costs, time of Covered Entity personnel, and reasonable attorneys' fees, costs and disbursements of legal counsel) arising from, related to, or in connection with any Incident involving PHI in Business Associate's possession, custody, or control, or any other breach of this agreement. This indemnity shall not be construed to limit Covered Entity's rights, if any, to common law indemnity.

The obligations of Business Associate (the "**Indemnitor**") under this agreement to defend, indemnify and hold harmless Covered Entity (including its affiliates and subsidiaries), and their respective employees, representatives and agents (each, an "**Indemnitee**") shall be subject to the following: (a) the Indemnitee shall provide the Indemnitor with prompt notice of the claim giving rise to such obligation; provided, however, that any failure or delay in giving such notice shall only relieve the Indemnitor of its obligation to defend, indemnify and hold the Indemnitee harmless to the extent it reasonably demonstrates that its defense or settlement of the claim or suit was adversely affected thereby; (b) the Indemnitor shall have control of the defense and of all negotiations for settlement of such claim or suit; provided, however, that the Indemnitee shall select counsel for such defense reasonably acceptable to Indemnitor with such consent not unreasonably withheld, delayed or conditioned and Indemnitor shall not settle any claim unless such settlement completely and forever releases the Indemnitee from all liability with respect to such claim and unless the Indemnitee consents to such settlement in writing (which consent shall not be unreasonably withheld); and (c) the Indemnitee shall cooperate with the Indemnitor in the defense or settlement of any such claim or suit; provided, however, that the Indemnitee shall be reimbursed for all reasonable out-of-pocket expenses incurred in providing any cooperation requested by the Indemnitor. Subject to clause (b) above, the Indemnitee may also participate in the defense of any claim or suit in which the Indemnitee is involved at its own expense.

M. **State Law.** Business Associate shall comply with state law confidentiality, privacy, security, document retention, and breach notification requirements involving "**Personal Information**" or "**Personally Identifiable Information**" (collectively, the "**PII**") as those terms are defined under state law, including but not limited to California Code section 1798.82. In this agreement, PII shall refer to any data elements that identify an Individual or that could be used to identify an Individual, including but not limited to an Individual's first name or initial and last name in combination with one or more of the following data elements: social security number; driver's license or state issued identification number; credit or debit card number; medical information (such as an Individual's condition, treatment, or payment information); financial information, such as checking account or other account number (either in

combination with a required security code, access code, or password that would permit access to the account, or alone if the account does not require such an access code); or other identifying information, such as e-mail addresses and usernames in combination with passwords or security questions, date of birth, mother's maiden name, digital signature, passport number, fingerprint or other biometric data, an insurance policy number, employment information, employment history, an employer, student, tribal, or military identification numbers.

Notwithstanding any provision to the contrary, the provisions of this agreement shall apply equally with respect to PII as they do to PHI; provided, however, that to the extent that state law is more stringent than the HIPAA Rules or the terms of this agreement, Business Associate agrees to comply with the requirement that provides more privacy and security protection to PII.

### **III. Covered Entity's Obligations.**

A. **Notice of Change in Privacy Practices.** Covered Entity shall notify Business Associate of any limitation(s) in Covered Entity's notice of privacy practices in accordance with 45 C.F.R. section 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

B. **Notice of Change in Permissions.** Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

C. **Notice of Change in Use.** Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. section 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

D. **Appropriate Requests.** Covered Entity shall not request that Business Associate use or disclose PHI in any manner that would not be permissible under the HIPAA Rules if done by Covered Entity.

### **IV. Term and Termination.**

A. **Term.** This is effective on the date stated in the introductory clause and will automatically terminate without any further action of the parties upon the termination or expiration of MOU.

B. **Termination for Cause.** If Covered Entity reasonably determines, in its sole discretion, that Business Associate has materially breached this agreement, Covered Entity may:

1. Provide Business Associate with 30 days written notice of the alleged material breach and an opportunity to cure the breach, immediately after which time this agreement and any Vendor Agreement under which Business Associate may create, receive, transmit, use, disclose, or maintain PHI for or on behalf of Covered Entity shall be automatically terminated if the breach is not cured; or
2. Immediately terminate this agreement and any Vendor Agreement under which Business Associate may create, receive, transmit, use, disclose, or maintain PHI for or on behalf of Covered Entity if cure is not possible; or
3. Report the violation to the Secretary if neither termination nor cure is feasible.

C. **Effect of Termination.** Upon termination or expiration of this agreement, Business Associate shall, at Covered Entity's option, return to Covered Entity or destroy all PHI in Business Associate's possession, and/or in the possession of any Subcontractor or agent of Business Associate. Business Associate shall not retain any copies of the PHI. In the event that return or destruction of the PHI is not feasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction of the PHI not feasible, and Covered Entity and Business Associate shall determine the terms and conditions under which Business Associate may retain the PHI. In such case, Business Associate shall extend the protections of this agreement to such PHI that is not returned or destroyed and limit further uses and disclosures of such PHI to those purposes that make the return or destruction not feasible for as long as Business Associate maintains such PHI. If Covered Entity elects destruction of the PHI, Business Associate shall certify in writing to Covered Entity that such PHI has been destroyed.

V. **Miscellaneous.**

A. **Amendments.** No amendment to this agreement will be effective unless it is in writing and signed by both parties. The parties shall amend this agreement as necessary to comply with the HIPAA Rules and state law.

B. **Interpretation.** Any ambiguity in this agreement shall be resolved to permit the parties to comply with the HIPAA Rules and state law.

C. **Choice of Law.** This agreement shall be governed in accordance with the laws of the state of California without regard to any conflict of laws principles.

D. **Audits, Inspection and Enforcement.** Upon request and with reasonable prior notice, Business Associate and its agents shall allow regulatory bodies to conduct a reasonable inspection of the facilities, systems, books, records, agreements, policies and procedures relating to the use or disclosure of PHI in accordance with this agreement or for the purpose of determining whether Business Associate is in compliance with its obligations under this agreement.

E. **Relationship to Agreements with Covered Entity.** In the event that a provision of this agreement is contrary to a provision of any other agreement between Business Associate and Covered Entity (including any inconsistencies in defined or capitalized terms), the most stringent provision shall control. The "most stringent provision" means the provision that provides the greatest privacy and security protection for PHI and that best permits compliance with the HIPAA Rules and state law.

F. **Survival.** Business Associate's obligations under section II.F.4 and section IV.C of this agreement shall survive the termination of this agreement.

G. **Waiver.** No delay or omission by Covered Entity in exercising any right or power under this agreement shall impair such right or power or be construed to be a waiver. Any decision by Covered Entity not to enforce a breach of this agreement shall not be construed to be a waiver of any succeeding breach.

H. **No Third Party Beneficiaries.** Nothing express or implied in this agreement is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Business Associate and their respective successors and assigns, any rights, remedies, obligations or liabilities whatsoever.

I. **Due Diligence.** Business Associate shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this agreement and is in compliance with the HIPAA Rules and state law.

J. **Judicial or Administrative Proceeding.** Business Associate shall notify Covered Entity if it is named as a defendant in a criminal proceeding for a violation of the HIPAA Rules.

Signature Page Follows

## BUSINESS ASSOCIATE AGREEMENT

### Signature Page

The parties are signing this agreement effective on the date stated in the introductory clause.

County of Monterey, a political subdivision of the State of California, on behalf of the Monterey County Health Department

Santa Cruz-Monterey-Merced Managed Medical Care Commission, doing business as Central California Alliance for Health

By: \_\_\_\_\_

By:  \_\_\_\_\_

Print Name: \_\_\_\_\_

Print Name: Stephanie Sonnenshine

Title: \_\_\_\_\_

Title: CEO

Date Signed: \_\_\_\_\_

Date Signed: 8/20/18

Address and Facsimile Number for Notices:

Address and Facsimile Number for Notices:

ATTN:

ATTN: Compliance Director

ATTN: Privacy Compliance Officer/Administration Bureau

Central California Alliance for Health

Company Name: Monterey County Health Department

1600 Green Hills Road, Ste. 101

Street: 1270 Natividad Road

Scotts Valley, CA 95066

City, State ZIP: Salinas, CA 93906

Facsimile Number: 831-430-5829


Facsimile Number: 831-796-8645

City, State ZIP: \_\_\_\_\_


Facsimile Number:

( ) \_\_\_\_\_

Reviewed as to fiscal provisions

  
Auditor-Controller  
County of Monterey 8/30/18

APPROVED AS TO FORM

  
COUNTY CLERK  
COUNTY OF MONTEREY

## APPENDIX A – ADDITIONAL SECURITY REQUIREMENTS

Business Associate shall implement a written information privacy and security program (which must be provided to Covered Entity upon reasonable request) that meets safeguard requirements stated in section II.B and that implements steps to ensure the continuous security of all computerized data systems containing PHI and PII (as defined in section II.M). Such steps shall include, at a minimum:

- Complying with all of the data system security precautions listed below in this Appendix A;
- Achieving and maintaining compliance with 45 C.F.R. Parts 160 and 164, subparts A and C (collectively, the “**HIPAA Security Rule**”), as necessary in conducting operations on behalf of Covered Entity under this agreement;
- Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III - Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in federal agencies; and
- 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.

### **I. Personnel Controls**

- A. **Employee Training.** All workforce members who assist in the performance of functions or activities on behalf of Covered Entity, or access or disclose Covered Entity PHI or PII 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 years following termination of the Vendor Agreement under which Business Associate may create, receive, transmit, use, disclose, or maintain PHI for or on behalf of Covered Entity.
- 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 Covered Entity PHI or PII 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 Covered Entity PHI or PII. The confidentiality statement must be renewed annually. The Business Associate shall retain each person’s written confidentiality statement for Covered Entity’s inspection for a period of six years following termination of the MOU under which Business Associate may create, receive, transmit, use, disclose, or maintain PHI for or on behalf of Covered Entity.
- D. **Background Check.** Before a member of the workforce may access Covered Entity PHI or PII, 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 Business Associate shall retain each workforce member's background check documentation for a period of three years following termination of the MOU under which Business Associate may create, receive, transmit, use, disclose, or maintain PHI for or on behalf of Covered Entity.

- E. **Security Officer Designation.** Business Associate shall designate a Security Officer to oversee its data security program who shall be responsible for carrying out the requirements of this section and for communicating on security matters with Covered Entity.

## II. Technical Security Controls

- A. **Workstation/Laptop encryption.** All workstations and laptops that process and/or store Covered Entity PHI or PII must be encrypted using a FIPS 140-2 certified algorithm which is 128 bit or higher, such as Advanced Encryption Standard ("AES"). The encryption solution must be full disk unless approved by the Covered Entity's Security and/or Privacy Officer.
- B. **Server Security.** Servers containing unencrypted Covered Entity PHI or PII 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 Covered Entity PHI or PII required to perform necessary business functions may be copied, downloaded, or exported.
- D. **Removable media devices.** All electronic files that contain Covered Entity PHI or PII data must be encrypted when stored on any removable media or portable device (i.e., USB thumb drives, floppies, CD/DVD, Blackberry, backup tapes, etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128 bit or higher, such as AES.
- E. **Antivirus software.** All workstations, laptops and other systems that process and/or store Covered Entity PHI or PII 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 Covered Entity PHI or PII 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 Covered Entity PHI or PII. 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 24 hours. 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 Covered Entity PHI or PII must be wiped using the Gutmann or U.S. Department of Defense (DOD) 5220.22M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission of Covered Entity.
- I. System Timeout.** The system providing access to Covered Entity PHI or PII 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 Covered Entity PHI or PII 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 Covered Entity PHI or PII, or which alters Covered Entity PHI or PII. 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 Covered Entity PHI or PII is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least three years after occurrence.
- L. Access Controls.** The system providing access to Covered Entity PHI or PII must use role based access controls for all user authentications, enforcing the principle of least privilege.
- M. Transmission encryption.** All data transmissions of Covered Entity PHI or PII outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128 bit 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 PII in motion such as website access, file transfer, and e-mail.
- N. Intrusion Detection.** All systems involved in accessing, holding, transporting, and protecting Covered Entity PHI or PII 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 Covered Entity PHI or PII 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 Covered Entity PHI or PII must have a routine procedure in place to review system logs for unauthorized access.
- C. **Change Control.** All systems processing and/or storing Covered Entity PHI or PII must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

#### IV. Business Continuity / Disaster Recovery Controls

- A. **Emergency Mode Operation Plan.** Business Associate must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic Covered Entity PHI or PII 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.** Business Associate must have established documented procedures to backup Covered Entity PHI to maintain retrievable exact copies of Covered Entity PHI or PII. 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 Covered Entity PHI or PII should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of Covered Entity data.

#### V. Paper Document Controls

- A. **Supervision of Data.** Covered Entity PHI or PII 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. Covered Entity PHI or PII 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 Covered Entity PHI or PII is contained shall be escorted and Covered Entity PHI or PII shall be kept out of sight while visitors are in the area.
- C. **Confidential Destruction.** Covered Entity PHI or PII must be disposed of through confidential means, such as cross cut shredding and pulverizing.
- D. **Removal of Data.** Covered Entity PHI or PII must not be removed from the premises of Business Associate except with express written permission of Covered Entity.
- E. **Faxing.** Faxes containing Covered Entity PHI or PII 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 Covered Entity PHI or PII shall be sealed and secured from damage or inappropriate viewing of PHI or PII to the extent possible. Mailings which include 500 or more individually identifiable records of Covered Entity PHI or PII 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 Covered Entity to use another method is obtained.