The Standard Agreement between the County of San Diego and the California Department of Aging

Privacy and Information Security Provisions

Information Privacy and Security Provisions – AIS Contractors

Source: County of San Diego, Aging and Independence Services Standard Agreement with CA Dept of Aging, 17-18

A. Information Assets

The Contractor, and its Subcontractors/Vendors, shall have in place operational policies, procedures, and practices to protect State information assets, including those assets used to store or access Personal Health Information (PHI), Personal Information (PI) and any information protected under the Health Insurance Portability and Accountability Act (HIPAA), i.e., public, confidential, sensitive and/or personal identifying information) as specified in the State Administrative Manual, 5300 to 5365.3: Cal. Gov. Code § 11019.9, DGS Management Memo 06-12; DOF Budget Letter 06-34; and CDA Program Memorandum 07-18 Protection of Information Assets and the Statewide Health Information Policy Manual.

Information assets may be in hard copy or electronic format and may include but is not limited to:

1. Reports
2. Notes
3. Forms
4. Computers, laptops, cellphones, printers, scanners
5. Networks (LAN, WAN, WIFI) servers, switches, routers
6. Storage media, hard drives, flash drives, cloud storage
7. Data, applications, databases

B. Encryption of Computing Devices

The Contractor, and its Subcontractors/Vendors, are required to encrypt data collected under this Agreement that is confidential, sensitive, and/or personal information including data stored on all computing devices {including but not limited to, workstations, servers, laptops, personal digital assistants, notebook computers and backup media) and/or portable electronic storage media (including but not limited to, discs, thumb/flash drives, portable hard drives, and backup media).

C. Disclosure

1. The Contractor, and its Subcontractors/Vendors, shall ensure that all confidential, sensitive and/or personal identifying information is protected from inappropriate or unauthorized access or disclosure in accordance with applicable laws, regulations and State policies.
2. The Contractor, and its Subcontractors/Vendors, shall protect from unauthorized disclosure, confidential, sensitive and/or personal identifying information such as names and other identifying information concerning persons receiving services pursuant to this Agreement, except for statistical information not identifying any participant.

3. "Personal Identifying Information" shall include, but not be limited to: name; identifying number; social security number; state driver's license or state identification number; financial account numbers; and symbol or other identifying characteristic assigned to the individual, such as finger or voice print or a photograph.

4. The Contractor, and its Subcontractors/Vendors, shall not use confidential, sensitive and/or personal identifying information above for any purpose other than carrying out the Contractor's obligations under this Agreement. The Contractor and its Subcontractors are authorized to disclose and access identifying information for this purpose as required by OAA.

5. The Contractor and its Subcontractors/Vendors, shall not, except as otherwise specifically authorized or required by this Agreement or court order, disclose any identifying information obtained under the terms of this Agreement to anyone other than CDA without prior written authorization from CDA. The Contractor may be authorized, in writing, by a participant to disclose identifying information specific to the authorizing participant.

6. The Contractor, and its Subcontractors/Vendors, may allow a participant to authorize the release of information to specific entities, but shall not request or encourage any participant to give a blanket authorization or sign a blank release, nor shall the Contractor accept such blanket authorization from any participant.

D. Security Awareness Training

1. The Contractor's employees, Subcontractors/Vendors, and volunteers handling confidential, sensitive and/or personal identifying information must complete the required CDA Security Awareness Training module located at https://www.aging.ca.gov/ProgramsProviders/#Resources within thirty (30) days of the start date of the Contract/Agreement, within thirty (30) days of the start date of any new employee, Subcontractor, Vendor or volunteer's employment and annually thereafter.

2. The Contractor must maintain certificates of completion on file and provide them to CDA upon request.

E. Contractor Confidentiality Statement

The Contractor shall sign and return a Contractor/Vendor Confidentiality Statement (CDA 1024) form with this Agreement. This is to ensure that the Contractor is aware of, and agrees to comply with, their obligations to protect CDA information assets from unauthorized access and disclosure.

F. Security Incident Reporting

A security incident occurs when CDA information assets are or reasonably believed to have been accessed, modified, destroyed, or disclosed without proper authorization, or are lost or stolen. The Contractor, and its Subcontractors/ Vendors, must comply with Article 14 requirements pertaining to breach notification.

G. Security Breach Notifications

Notice must be given by the Contractor, and/or its Subcontractors/Vendors to anyone whose confidential, sensitive and/or personal identifying information could have been breached in accordance with HIPAA, the Information Practices Act of 1977, and State policy.

H. Software Maintenance

The Contractor, and its Subcontractors/Vendors, shall apply security patches and upgrades in a timely manner and keep virus software up-to-date on all systems on which State data may be stored or accessed.

I. Electronic Backups

The Contractor, and its Subcontractors/Vendors, shall ensure that all electronic information is protected by performing regular backups of files and databases and ensure the availability of information assets for continued business. The Contractor, and its Subcontractors/Vendors, shall ensure that all data, files and backup files are encrypted.

J. Provisions of this Article

The provisions contained in this Article shall be included in all contracts of both the Contractor and its Subcontractors/Vendors where either PHI, confidential, personal, or sensitive information is obtained during the course of carrying out the obligations of this Agreement or any sub-Agreements related to the services required in this Agreement.

K. Copyrights

1. If any material funded by this Agreement is subject to copyright, the State reserves the right to copyright such material and the Contractor agrees not to copyright such material, except as set forth in "Rights in Data" Section of this Article.

2. The Contractor may request permission to copyright material by writing to the Director of CDA. The Director shall grant permission, or give reason for denying permission to the Contractor in writing within sixty (60) days of receipt of the request.

3. If the material is copyrighted with the consent of CDA, the State reserves a royalty-free, non-exclusive, and irrevocable license to reproduce, prepare derivative works, publish, distribute and use such materials, in whole or in part, and to authorize others to do so, provided written credit is given to the author.

4. The Contractor certifies that it has appropriate systems and controls in place to ensure that State funds will not be used in the performance of this contract for the acquisition, operation, or maintenance of computer software in violation of copyright laws.

L. Rights in Data

1. The Contractor shall not publish or transfer any materials, as defined in paragraph 2 below, produced or resulting from activities supported by this Agreement without the express written consent of the Director of CDA. That consent shall be given, or the reasons for denial shall be given, and any conditions under which it is given or denied, within thirty (30) days after the written request is received by CDA. CDA may request a copy of the material for review prior to approval of the request. This subsection is not intended to prohibit the Contractor from sharing identifying client information authorized by the participant or summary program information which is not client-specific.

   The Contractor shall not spend or encumber funds covered by this Agreement on research or publications; or any activities, staff, products, or materials, including analysis and services, supporting research, and publications, unless expressly authorized by the terms of this Agreement. The Contractor shall not publish any document or materials produced or resulting from activities supported by this Agreement unless the copy of the final draft for publication has been sent to the Director of CDA, for approval, at least sixty (60) days before it is to be printed.

2. As used in this Agreement, the term "subject data" means writings, sound recordings, pictorial reproductions, drawings, designs or graphic representations, procedural manuals, forms, diagrams, workflow charts, equipment descriptions, data files and data processing or computer programs, and works of any similar nature (whether or not copyrighted or copyrightable) which are first produced or developed under this Agreement. The term does not include financial reports, cost analyses, and similar information incidental to contract administration, or the exchange of that information between AAAs to facilitate uniformity of contract and program administration on a statewide basis.

3. Subject only to other provisions of this Agreement, the State may use, duplicate, or disclose in any manner, and have or permit others to do sosubject to State and federal Jaw, all subject data delivered under this Agreement.

4. Materials published by or transferred to the Contractor shall: (a) contract from the CDA; (b) give the name of the state "The materials or product were a result of a project funded by an entity the address, and telephone number at which the supporting data is available"; and (c) Include a statement that "The conclusions and opinions expressed may not be those of the California Department of Aging, and that the publication may not be based upon or inclusive of all raw data."

M. Health Insurance Portability and Accountability Act (HIPAA)

As applicable, The Contractor agrees to comply with the privacy and security requirements of HIPAA~~, and~~ ensure that Subcontractors/Vendors comply with the privacy and security requirements of HIPAA, and comply with the requirements in this section M, including:

1. This Contract (Agreement) has been determined to 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").

2. The Department of Health Care Services ("DHCS") wishes to disclose to 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.

3. As set forth in this Agreement, Contractor, here and after, is the Business Associate of DHCS acting on DHCS' behalf and provides services, arranges, performs or assists in the performance of functions or activities on behalf of DHCS and creates, receives, maintains, transmits, uses or discloses PHI and PI. DHCS and Business Associate are each a party to this Agreement and are collectively referred to as the "parties."

4. 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 DHCS 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.

5. 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.

6. Definitions

   a. Breach shall have the meaning given to such term under HIPAA, the HITECH Act, the HIPAA regulations, and the Final Omnibus Rule.

   b. Business Associate shall have the meaning given to such term under HIPAA, the HITECH Act, the HIPAA regulations, and the final Omnibus Rule.

   c. Covered Entity shall have the meaning given to such term under 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.

   h. Personal Information shall have the meaning given to such term In California Civil Code section 1798.29.

   i. Protected Health Information means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or is transmitted or maintained In any other form •Jr medium, as set forth under 45 CFR section 160.103.

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 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.

n. Unsecured PHI shall have the meaning given to such term under the HITECH Act, 42 U.S.C. section 17932(h),any guidance issued pursuant to such Act, and the HIPAA regulations.

7. 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 DHCS, provided that such use or disclosure would not violate the HIPAA regulations, if done by DHCS. 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.

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

1) 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.

2) Provision of Data Aggregation Services. Use PHI to provide data aggregation services to DHCS. Data aggregation means the combining of PHI created or received by the Business Associate on behalf of DHCS 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 DHCS.

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 DHCS 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 PHI, including electronic PHI, that it creates, receives, maintains, uses or transmits on behalf of DHCS, 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 privacy and security 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. Business Associate will provide DHCS with Its current and updated policies.

3) **Security**. To take any and all steps necessary to ensure the continuous security of all 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), as necessary In conducting operations on behalf of DHCS under this Agreement;

   c) 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 OMS Circular No. A-130, Appendix III - Security of Federal Automated Information Systems, which sets forth guidelines for automated Information systems in Federal agencies; and

   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.

   e) 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 DHCS.

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 DHCS, 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 are 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 Is directly liable and subject to civil penalties for falling 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 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 an opportunity for the subcontractor to cure the breach or end the violation and terminate the agreement if the subcontractor does not cure the breach or end the violation within the time specified by DHCS; or

   b) 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 DHCS may require, and in the time and manner designated by DHCS (upon reasonable notice and during Business Associate's normal business hours) to PHI in a Designated Record Set, to DHCS (or, as directed by DHCS), to an Individual, in accordance with 45 CFR section 164.524. Designated Record Set means the group of records maintained for DHCS that includes medical, dental and bill ng records about individuals; enrollment, payment, claims adjudication, and case or medical management systems maintained for DHCS health plans; or those records used to make decisions about individuals on behalf of DHCS. Business Associate shall use the forms and processes developed by DHCS for this purpose and shall respond to requests for access to records transmitted by DHCS 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 DHCS 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 DHCS that was provided to DHCS by the Social Security Administration, upon request by DHCS, Business Associate shall provide DHCS 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 PHIthat DHCS directs or agrees to pursuant to 45 CFR section 164.526, In the time and manner designated by DHCS.

h. **Internal Practices.** To make Business Assoc1ate'sInternal practices, books and records relating to the use and disclosure of PHI received from DHCS, or created or received by Business Associate on-behalf of DHCS, available to DHCS or to the Secretary of the U.S. Department of Health and Human Services in a time and manner designated by DHCS or by the Secretary, for purposes of determining DHCS' compliance with the HIPM regulations. If any information needed for this purpose is in the exclusive possession of any other entity or person and the other entity or person falls or refuses to furnish the Information to Business Associate, Business Associate shall so certify to DHCS and shall set forth the efforts it made to obtain the information.

i. **Documentation of Disclosures**. To document and make available to DHCS or (at the direction of DHCS) to an Individual 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 DHCS 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 DHCS 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 systems for the discovery and prompt reporting of any breach or security incident, and to take the following steps:

1) Upon discovery of a breach or suspected security incident, Intrusion 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 applicable Federal and State laws and regulations.

c) Report the incident to the County as specified in Article 14.

2) Notification of Individuals. If the cause of a breach of PHI or PI is attributable to Business Associate or its subcontractors, agents or vendors, Business Associate shall notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal law and shall pay any costs of such notifications, as well as any costs 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 DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made.

3) 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 all required reporting 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 notify the Secretary of the breach immediately upon discovery of the breach.

k. **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.

l. **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 HfPAA, the HITECH Act and the HIPAA regulations.

8. Audits, Inspection and Enforcement

a. From time to time, DHCS may inspect the facilities, systems, books and records of Business Associate to monitor compliance with this Agreement and this Addendum. Business Associate shall promptly remedy any violation of any provision of this Addendum and shall certify the same to the DHCS Privacy Officer in writing. The fact that DHCS inspects, or fails to inspect, or has the right to inspect, Business Associate's facilities, systems and procedures does not relieve Business Associate of its responsibility to comply with this Addendum, nor does DHCS':

1) Failure to detect or

2) Detection, but failure to notify Business Associate or require Business Associate's remediation of any unsatisfactory practices constitute acceptance of such practice or a waiver of DHCS' 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 notify DHCS and provide DHCS 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. Business Associate is responsible for any civil penalties assessed due to an audit or Investigation of Business Associate, In accordance with 42 U.S.C.section 17934(c).

9. 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 DHCS to Business Associate, or created or received by Business Associate on behalf of DHCS, Is destroyed or returned to DHCS, in accordance with 45 CFR 164.504(e)(2)(li)(I).

b. Termination for Cause. In accordance with 45 CFR section 164.504(e)(1)(11), upon DHCS' knowledge of a material breach or violation of this Addendum by Business Associate, DHCS 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 DHCS; 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 notify DHCS if it is named as a defendant in a criminal proceeding for a violation of HIPAA. DHCS may terminate this Agreement if Business Associate Is found guilty of a criminal violation of HIPAA. DHCS may terminate this Agreement if a finding or stipulation that the Business Associate has violated any standard or requirement of HIPAA, or other security or privacy laws 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 DHCS (or created or received by Business Associate on behalf of DHCS) 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 DHCS of the conditions that make the return or destruction Infeasible, and DHCS 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.

10. Miscellaneous Provisions

a. Disclaimer. DHCS 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 are rapidly evolving and that amendment of this Addendum may be required to provide for procedures

to ensure compliance with such developments. The parties specifically agree to take such action as Is necessary to implement the standards and requirements of HIP. the HITECH Act, the HIPAA regulations and other applicable laws relating to the security or privacy of PHI. Upon OHCS' request, Business Associate agrees to promptly enter into negotiations with DHCS 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. DHCS may terminate this Agreement 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 DHCS pursuant to this Section; or

2) Business Associate does not enter into an amendment providing assurances regarding the safeguarding of PHI that DHCS 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 make itself and any subcontractors, employees or agents assisting Business Associate in the performance of its obligations under this Agreement, available to DHCS at no cost to DHCS to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against DHCS, its directors, officers or employees based upon claimed violation of HIPAA, the HIPAA regulations or other laws relating to security and privacy, which Involves inactions or actions by the Business Associate, except where Business Associate or Its subcontractor, employee or agent Is a named adverse 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 DHCS 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 "Effect of Termination" Section above ~~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.

11. Privacy and Security Controls

a. Personnel Controls

1) **Employee Training**. All workforce members who assist in the performance of functions or activities on behalf of DHCS, or access or disclose DHCS 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.

2) **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.

3) **Confidentiality Statement**. All persons that will be working with DHCS 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 DHCS PHI or PI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for DHCS inspection for a period of six (6) years following contract termination.

4) **Background Check**. Before a member of the workforce may access DHCS 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.

b. Technical Security Controls

1) **Workstation/Laptop encryption**. All workstations and laptops that process and or store DHCS 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 DHCS Information Security Office.

2) **Server Security**. Servers containing unencrypted DHCS 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.

3) **Minimum Necessary**. Only the minimum necessary amount of DHCS PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.

4) **Removable media devices**. All electronic files that contain DHCS PHI or PI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, smartphones, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which Is 128blt or higher, such as AES.

5) **Antivirus software**. All workstations, laptops and other systems that process and/or store OHCS PHI or PI must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

6) **Patch Management**. All workstations, laptops and other systems that process and/or store DHCS 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.

7) **User IDs and Password Controls**. All users must be issued a unique user name for accessing DHCS 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 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)

8) **Data Destruction**. When no longer needed, all DHCS 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.

9) **System Timeout**. The system providing access to DHCS PHI or PI must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.

10) **Warning Banners**. All systems providing access to DHCS 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.

11) **System Logging.** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for DHCS PHI or PI, or which alters DHCS 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 DHCS PHI or PI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.

12) **Access Controls.** The system providing access to DHCS PHI or PI must use role based access controls for all user authentications, enforcing the principle of least privilege.

13) **Transmission encryption.** All data transmissions of DHCS 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.

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

c. Audit Controls

1) **System Security Review**. All systems processing and/or storing DHCS 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.

2) **Log Reviews**. All systems processing and/or storing DHCS PHI or PI must have a routine procedure in place to review system logs for unauthorized access.

3) **Change Control**. All systems processing and/or storing DHCS PHI or PI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, Integrity and availability of data.

d. Business Continuity I Disaster Recovery Controls

1) **Emergency Mode Operation Plan**. Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic DHCS 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.

2) **Data Backup Plan**. Contractor must have established documented procedures to backup DHCS PHI to maintain retrievable exact copies of DHCS PHI or PI. 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 DHCS PHI or PI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of DHCS data.

e. Paper Document Controls

1) **Supervision of Data**. DHCS PHI or PI in paper form shall not be left unattended at any time, unless it Is locked In a fife cabinet, fi e room, desk or office. Unattended means that Information Is not being observed by an employee authorized to access the information. DHCS 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.

2) **Escorting Visitors**. Visitors to areas where DHCS PHI or PI is contained shall be escorted and DHCS PHI or PI shall be kept out of sight while visitors are in the area.

3) **Confidential Destruction**. DHCS PHI or PI must be disposed of through confidential means, such as cross cut shredding and pulverizing.

4) **Removal of Data**. DHCS PHI or PI must not be removed from the premises of the Contractor except with express written permission of DHCS.

5) **Faxing**. Faxes containing DHCS 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.

6) **Mailing**. Mailings of DHCS PHI or PI 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 DHCS 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 DHCS to use another method fs obtained.