Recitals – STANDARD RISK

A. This Contract (Agreement) constitutes a business associate relationship under the Health Insurance Portability and Accountability Act (HIPAA) and its implementing privacy and security regulations at 45 C.F.R. Parts 160 and 164 (collectively, the HIPAA regulations).

B. The California Department of Corrections and Rehabilitation, California Correctional Health Care Services (CCHCS) wishes to disclose to Business Associate certain information pursuant to the terms of this Agreement, some of which may constitute Protected Health Information (PHI) and confidential information protected by Federal and/or state laws.

C. Protected Health Information or PHI means any information, whether oral or recorded in any form or medium that relates to the past, present, or future physical or mental condition of an individual, the provision of health and dental care to an individual, or the past, present, or future payment for the provision of health and dental care to an individual; and that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. PHI shall have the meaning given to such term under HIPAA and HIPAA regulations, as the same may be amended from time to time. Confidential Information means information protected by Federal and/or state laws identified in this Agreement.

D. Unsecured Protected Health Information means protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified in guidance from the Secretary of the U.S. Department of Health and Human Services (Secretary).

E. Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of CCHCS PHI or interference with system operations in Business Associate's information system.

F. As set forth in this Agreement, the Contractor is the Business Associate of CCHCS that provides services, medical items for identified patients, arranges, performs or assists in the performance of functions or activities on behalf of CCHCS and creates, receives, maintains, transmits, uses or discloses PHI.

G. CCHCS and Business Associate desire to protect the privacy and provide for the security of PHI and confidential information created, received, maintained, transmitted, used or disclosed pursuant to this Agreement, in compliance with HIPAA, HIPAA regulations, and other applicable laws.

H. The purpose of the Business Associate Agreement (BAA) is to satisfy certain standards and requirements of HIPAA and the HIPAA regulations.

I. The terms used in this Agreement, but not otherwise defined, shall have the same meanings as those terms in the HIPAA regulations.

In exchanging information pursuant to this Agreement, the parties agree as follows:

1. Permitted Uses and Disclosures of PHI by Business Associate

A. ***Permitted Uses and Disclosures***. Except as otherwise indicated in this Agreement, Business Associate may use or disclose PHI only to perform functions, activities or services specified in this Agreement or as necessary to perform Business Associates obligation's under the Agreement to which this Business Associate Agreement is attached, for, or on behalf of CCHCS, provided that such use or disclosure would not violate the HIPAA regulations, if done by CCHCS.

B. ***Specific Use and Disclosure Provisions.*** Except as otherwise indicated in this Agreement, 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 or to carry out the legal responsibilities of the Business Associate, provided that 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 CCHCS. Data aggregation means the combining of PHI created or received by the Business Associate on behalf of CCHCS 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 CCHCS.

3) De-identify any and all PHI received by Business Associate under this Business Associate Agreement, provided that the de-identification conforms to the requirements of the Privacy Rule.

2. Responsibilities of Business Associate

Business Associate agrees:

A. ***Nondisclosure.*** Not to use or disclose PHI other than as permitted or required by this Agreement or as required by law. Business Associate acknowledges that in some circumstances, Business Associate's (BA) staff or contractors working on certain confidential or sensitive CCHCS projects relating to correctional security may be requested to execute a non-redisclosure agreement with respect to such confidential or sensitive information which may not be redisclosed. If a non-redisclosure statement is signed by any BA staff or contractor, such document shall be retained by the BA for 6 (six) years following termination of the contract timeframe to which this BAA is attached.

B. ***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 CCHCS; and to prevent use or disclosure of PHI other than as provided for by this Agreement. 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 C, Security, below. Upon written request, Business Associate will provide CCHCS with an attestation that its current and regularly updated internal privacy and information security policies comply with this requirement. And, if applicable, to the extent Business Associate stores CCHCS PHI, CCHCS retains the right to inspect Business Associate's information privacy and security program if Business Associate does not provide an attestation within a reasonable timeframe to respond to the attestation request.

C. ***Security.*** To take the reasonably necessary steps to ensure the continuous security of all computerized data systems containing Covered Entity's PHI, and provide data security procedures for the use of CCHCS at the end of the contract period. These steps shall include, at a minimum:

1) Complying with all of the data system security precautions listed in this Agreement or in an Exhibit incorporated into this Agreement; and

2) To the extent applicable, achieve and maintain compliance with the HIPAA Security Rule (45 CFR Parts 160 and 164), in conducting operations on behalf of CCHCS under this agreement.

3) If Business Associate stores CCHCS PHI, Business Associate will comply with the safeguard provisions provided at https://www.dgs.ca.gov/Resources/SAM/TOC/5300/5300-5 as provided in the Department's Information Security Policy, embodied in the Security and Risk Management Policy in the Information Technology Section of the State Administrative Manual (SAM), § 4840 et seq., Information Security Policy in SAM § 5300, et. seq. and State Information Management Manual (SIMM) § 5300 et. seq. If the above safeguard standards change, and after Business Associate receives notice of any changes, Business Associate agree to work in good faith to determine if Business Associate can comply with the changes, and if Business Associate determines that it cannot comply with the changes, CCHCS and Business Associate agree that this Business Associate agreement and underlying agreements with CCHCS may be immediately terminated by either party.

4) Background Check. Before a member of the workforce may access CCHCS PHI and depending on the nature of the scope of work, a thorough background check of that workforce member may be conducted (i.e. LiveScan), with evaluation of the results to assure that there is no indication that the workforce member 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.

5) Business Associate shall designate an Information 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 CCHCS.

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

E. ***Business Associate's Agents***. If Business Associate subcontracts the services under the agreement to which this Business Associate Agreement is attached, ensure that any agents, including subcontractors, to whom Business Associate provides PHI received from or created or received by Business Associate on behalf of CCHCS, agree to the same restrictions and conditions that apply to Business Associate with respect to such PHI, including implementation of reasonable and appropriate administrative, physical, and technical safeguards to protect such PHI; and to incorporate, when applicable, the relevant provisions of this Agreement into each subcontract or with agents or subcontractors.

F. ***Availability of Information to* CCHCS *and Individuals***. To provide access as CCHCS may require, and in the time and manner designated by CCHCS (upon reasonable notice and during Business Associate's normal business hours) to PHI in a Designated Record Set, to CCHCS (or, as directed by CCHCS), to an Individual, in accordance with 45 C.F.R. § 164.524. Designated Record Set means the group of records maintained for CCHCS that includes medical, dental and billing records about individuals; enrollment, payment, claims adjudication, and case or medical management systems maintained for CCHCS health plans; or those records used to make decisions about individuals on behalf of CCHCS. Business Associate shall use the forms and processes developed by CCHCS for this purpose and shall respond to requests for access to records transmitted by CCHCS within fifteen (15) calendar days of receipt of the request by producing the records or verifying that there are none.

G. ***Amendment of PHI***. To make any amendment(s) to PHI that CCHCS directs or agrees to pursuant to 45 C.F.R. § 164.526, in the time and manner designated by CCHCS.

H. ***Internal Practices***. To make Business Associate's internal practices, books and records relating to the use and disclosure of PHI received from CCHCS, or created or received by Business Associate on behalf of CCHCS, available to CCHCS or to the Secretary in a time and manner designated by CCHCS or by the Secretary, for purposes of determining CCHCS compliance with the HIPAA regulations.

I. ***Documentation of Disclosures***. To document and make available to CCHCS (within 14 calendar days) or (at the direction of CCHCS) 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 45 C.F.R. § 164.528.

J. ***Notification of Patient Confidential Communications.*** Notify CCHCS within two (2) business days of any patient (or patient's representative) preferences (or changes to) regarding method of or how to communicate with the patient.

K. ***Notification of Information Security Incidents, Investigation, and Written Reporting***.

1) ***Discovery of Information Security Incident***. To notify CCHCS ***immediately by telephone call plus email/electronic communication*** upon the discovery of an information security incident involving the privacy of or security of PHI in computerized form if the PHI was, or is reasonably believed to have been, acquired by an unauthorized person, or ***within 24 hours by email/electronic communication*** of any suspected security incident, intrusion or unauthorized use or disclosure of PHI in violation of this Agreement, or potential loss of confidential data affecting this Agreement. Notification shall be provided to the CCHCS contract manager, the CCHCS Privacy Officer, and the CCHCS Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves electronic PHI, notification shall be provided by calling the CCHCS ITSD Solution Center at **1-888-735-3470**. Business Associate shall take:

   i. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment, including potential claims or exemptions or exceptions following mitigation; and

   ii. Any and all actions pertaining to such unauthorized disclosures required by applicable Federal and State laws and regulations.

2) ***Investigation of Information Security Incident and Status Reporting to CCHCS***. To immediately investigate such information security incident, breach, or unauthorized use or disclosure of PHI. Within 72 hours of the discovery, to notify and provide the status of the investigation to the CCHCS contract manager(s), the CCHCS Privacy Officer, and the CCHCS Information Security Officer of:

   i. What data elements were involved and the extent of the data involved in the breach,

   ii. A description of the unauthorized persons known or reasonably believed to have improperly used, disclosed, or received PHI,

   iii. A description of where the PHI is believed to have been improperly transmitted, sent, or utilized,

   iv. A description of the probable causes of the improper use or disclosure; and

   v. Whether Civil Code § 1798.29 or § 1798.82 or any other federal or state laws requiring individual notifications of breaches are triggered.

   Notwithstanding the above, Business Associate shall not be obligated to report unsuccessful attempts to penetrate computer networks or servers that do not result in loss of data or degradation of computer networks or services, unless, if applicable,Business associate stores CCHCS PHI and the unsuccessful attempts involves CCHCS PHI.

3) ***Written Report***. To provide an initial written report of the investigation to the CCHCS contract managers, the CCHCS Privacy Officer, and the CCHCS Information Security Officer within ten (10) calendar days of the information security incident, discovery of the breach, or discovery of unauthorized use, disclosure, or receipt. The report shall be in the form and manner required by CCHCS and includes, but is not limited to, the information specified above, as well as a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. The initial report shall be submitted using the CCHCS Information Security Incident Report for external entities (ISIR) available at https://cchcs.ca.gov/wp-content/uploads/sites/60/ITSD/CCHCS-ISIR.pdf.

   The ISIR shall be emailed to the CCHCS Information Security Office at CCHCS-ISO@cdcr.ca.gov. Business Associate shall provide reasonable cooperation and work with CCHCS in good faith as the investigation progresses, and at the request of CCHCS. CCHCS retains all rights as the Covered Entity to review the sufficiency of the BA's proposed notice, investigation activities regarding CCHCS PHI incidents, or reporting of information security incidents involving CCHCS PHI.

4) ***Notification of Individuals***. To the extent a determination has been made that patient notification is required in a breach involving Business Associate, the parties agree to work together in good faith to determine the responsible party and any cost associated with such notification. Provided however, nothing shall excuse the obligations on the Business Associated as required under law. Business Associate shall pay any such costs of notifications or the costs associated with the breach if the breach is determined to be solely the responsibility of the Business Associate or their subcontractor. The CCHCS contract managers, the CCHCS Privacy Officer, and the CCHCS Information Security Officer shall approve the time, manner and content of any such notifications prior to release of the notification. When a determination is made that patient notification is required in a breach involving Business Associate, both parties agree to cooperate on the notification language.

5) CCHCS ***Contact Information***. To direct communications to the above referenced CCHCS staff, the Contractor shall initiate contact as indicated herein CCHCS 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 Agreement.

CCHCS	CCHCS	CCHCS
Contract Manager	**Privacy Officer**	**Information Security Officer**
See Exhibit A for Contract Manager information See the Scope of Work exhibit for Program Contract Manager Information	Privacy Officer California Correctional Health Care Services P.O. Box 588500, Bldg. D3, Elk Grove, CA 95758 Email: Privacy@cdcr.ca.gov Telephone: 1-877-974-4722	Information Security Officer Information Security Officer CCHCS Information Technology Services Division P.O. Box 588500, Bldg. C3, Elk Grove, CA 95758 Email: CCHCS-ISO@cdcr.ca.gov Telephone: 916-691-3243

L. ***Employee Training and Discipline***. If Business Associate requires access to CCHCS's systems, then Business Associate agrees to train and use reasonable measures to ensure compliance with the

requirements of this Agreement by employees who assist in the performance of functions or activities on behalf of CCHCS under this Agreement and use or disclose PHI and discipline such employees who intentionally violate any provisions of this Agreement, including additional training, progressive discipline, removal, or up to and including termination if warranted by the facts. In complying with the provisions of this section L, Business Associate shall observe the following requirements:

1) Business Associate shall provide information privacy and security training, at least every twelve (12) calendar months, at its own expense, to all its employees who assist in the performance of functions or activities on behalf of CCHCS under this Agreement and use or disclose PHI.

2) Business Associate shall document the employee's name and the date on which the training was completed and retain such documentation. Upon written request of CCHCS, Business Associate shall certify to CCHCS that such employees that provide services under the Agreement to which this Business Associate Agreement is attached have completed the training indicated above for CCHCS inspection for a period of three years following contract termination, and shall provide copies of training certifications to CCHCS on request.

3. Obligations of CCHCS

CCHCS agrees to:

A. ***Notice of Privacy Practices***. Provide Business Associate with the Notice of Privacy Practices that CCHCS produces in accordance with 45 C.F.R. § 164.520, as well as any changes to such notice. To ensure Notice of Privacy Practices to patients allows for the provisions of PHI to Business Associate.

B. ***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. If Business Associate staff or contractors execute a non-redisclosure agreement pursuant to section 2A above, CCHCS shall review those agreements on an annual basis to determine whether such access remains appropriate.

C. ***Notification of Restrictions***. Notify the Business Associate of any restriction to the use or disclosure of PHI that CCHCS has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect the Business Associate's use or disclosure of PHI.

D. ***Notification of Patient Confidential Communications.*** Notify the Business Associate (within 2 calendar days of request) of any patient (or patient's representative) preferences (or changes to) regarding the method of or how to communicate with the patient.

E. ***Requests Conflicting with HIPAA Rules***. Not request the Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA regulations.

4. Audits, Inspection and Enforcement

If Business Associate saves or stores CCHCS PHI on Business Associate's systems, then from time to time, CCHCS may request, and Business Associate shall provide, the necessary information, books, and records of Business Associate pertaining to CCHCS PHI to enable CCHCS to monitor compliance with this Agreement. Business Associate shall promptly remedy any violation of any provision of this Agreement and shall certify the same to the CCHCS Privacy Officer in writing. The fact that CCHCS, or its state oversight agency or federal oversight agency inspects, or fails to inspect, or has the right to inspect Business Associate does not relieve Business Associate of its responsibility to comply with this Agreement, nor does CCHCS':

A. Failure to detect; or

B. Detection, but failure to notify Business Associate or require Business Associate's remediation of any unsatisfactory practices does not constitute acceptance of such practice or a waiver by CCHCS of any of its inspection and/or enforcement rights under this Agreement.

Business Associate may meet this requirement by providing a SOC2 certificate of compliance or other certificate of compliance to nationally recognized information security standards and procedures by an accreditation body acceptable to CCHCS. Business Associate shall ensure SOC2 or other compliance certificates are valid and in effect for the duration of any contract to which this BAA attaches.

5. Termination

A. ***Termination for Cause****.* Upon CCHCS knowledge of a material breach of this Agreement by Business Associate, CCHCS 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 CCHCS;

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

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

B. ***Judicial or Administrative Proceedings****.* Business Associate will notify CCHCS if it is named as a defendant in a criminal proceeding for a violation of HIPAA. CCHCS may terminate this Agreement if Business Associate is found guilty of a criminal violation of HIPAA. CCHCS 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.

C. ***Effect of Termination****.* Upon termination or expiration of this Agreement for any reason, Business Associate shall return or destroy all PHI received from CCHCS (or created or received by Business Associate on behalf of CCHCS) that Business Associate still maintains in any form, and shall retain no copies of such PHI or, if return or destruction is not feasible, shall continue to extend the protections of this Agreement to such information, 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.

6. Miscellaneous Provisions

A. ***Disclaimer****.* CCHCS makes no warranty or representation that compliance by Business Associate with this Agreement, 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 the safeguarding of PHI solely transferred to it under applicable federal or state law.

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 Agreement may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such

action as necessary to implement the standards and requirements of HIPAA, the HIPAA regulations and other applicable laws relating to the security or privacy of PHI. Upon CCHCS request, Business Associate agrees to promptly enter into negotiations with CCHCS concerning an amendment to this Agreement confirming written assurances consistent with the standards and requirements of HIPAA, the HIPAA regulations or other applicable laws. CCHCS 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 Agreement when requested by CCHCS pursuant to this Section, or

2) Business Associate does not enter into an amendment providing assurances regarding the safeguarding of PHI that CCHCS 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****.* If Business Associate stores CCHCS PHI*,* Business Associate shall make itself available, and, if applicable, any subcontractors, employees or agents assisting Business Associate in the performance of its obligations under this Agreement, relating to the Business Associate's internal practices, books and records relating to the Use and Disclosure of PHI received from or created or received by Business Associate on behalf of CCHCS to the Secretary of HHS, and if Business Associate stores CCHCS PHI to CDII, CDPH, or other administrative oversight proceeding or litigation, for the purposes of determining CCHCS' or the Business Associate's compliance with the Privacy Rule, the Security Rule, and the Breach Notification Rule, subject to any applicable legal privileges.

D. ***No Third-Party Beneficiaries****.* Nothing express or implied in the terms and conditions of this Agreement is intended to confer, nor shall anything herein confer, upon any person other than CCHCS or Business Associate and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

E. ***Interpretation*****.** The terms and conditions in this Agreement shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HIPAA regulations and applicable state laws. The parties agree that any ambiguity in the terms and conditions of this Agreement shall be resolved in favor of a meaning that complies and is consistent with HIPAA and the HIPAA regulations.

F. ***Regulatory References****.* A reference in the terms and conditions of this Agreement to a section in the HIPAA regulations means the section in effect or as amended during the Agreement term.

G. ***Survival****.* The respective rights and obligations of Business Associate under Section 6.C of this Agreement 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.