HIPAA BUSINESS ASSOCIATE AGREEMENT

# **DEFINITIONS**

## Catch-all definition:

1. The following terms and others used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use[[1]](#footnote-1)

## Specific definitions:

1. Business Associate.  “Business Associate” shall generally have the same meaning as the term “business associate” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean the Contractor to the contract to which this Business Associate Agreement is attached as an exhibit. For purposes of this exhibit only, the term “Agreement” shall refer to this Business Associate Agreement. The term “Service Agreement” shall refer to the contract to which this Business Associate Agreement is attached as an exhibit.
2. Covered Entity.  “Covered Entity” shall generally have the same meaning as the term “covered entity” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean California Department of Corrections and Rehabilitation, California Correctional Health Care Services (CCHCS).
3. HIPAA Rules.  “HIPAA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.
4. Confidential Information. “Confidential Information” shall mean any and all non-public, medical, financial and personal information in whatever form (written, oral, visual, or electronic) possessed or obtained by either party. Confidential Information shall include all information which (i) either party has labeled in writing as confidential, (ii) is identified at the time of disclosure as confidential, (iii) is commonly regarded as confidential in the health care industry, or (iv) is Protected Health Information as defined by HIPAA.

# **PERMITTED USES AND DISCLOSURES**

1. Specific Use and Disclosure Provisions. Except as otherwise indicated in this Agreement Business Associate may:
2. Use and disclose for management and administration. Use and disclose Protected Health Information (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 was aware that the confidentiality of the information has been breached.
3. Provision of Data Aggregation Services. Use PHI to provide data aggregation services to California Correctional Health Care Services (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 analyses that relate to the health care operations of CCHCS.

# **PROHIBITED USES AND DISCLOSURES**

1. Specific Prohibitions on Disclosures. Except as otherwise indicated in this Agreement Business Associate may not:
2. Use or disclose PHI for payment. 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).
3. Sell or Exchange PHI for Remuneration. Business Associate shall not directly or indirectly receive remuneration in exchange for PHI, except with the prior written consent of CCHCS and as permitted by 42 U.S.C. section 17935(d) (2).
4. **OBLIGATIONS OF BUSINESS ASSOCIATE**
   1. Business Associate agrees:
      1. Nondisclosure. Not to use or disclose 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 CCHCS in compliance with 45 CFR sections 164.308, 164.310 and 165.312, 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 policy 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 CCHCS 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 personally identifiable information (PII), and to protect documents containing PHI and/or PII. These steps shall include, at a minimum.
         1. To comply with all data system security precautions listed in section IX, Business Associate Data Security Requirements.
         2. To achieve and maintaining compliance with the HIPAA Security Rule (45 CFR Parts 160 and 164), as necessary in conducting operations on behalf of CCHCS under this agreement.
         3. To provide a level and scope of security that is a 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
         4. 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.
         5. 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 CCHCS.
      4. 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 and its subcontractors in violation of the requirements of this Agreement.
      5. Duty of Business Associate to Comply with HIPAA When Associating with Agents and Subcontractors.
         1. Business Associate shall enter into written agreements with any agents, including subcontractors and vendors, to whom Business Associates provides PHI or PII received from or created or received by Business Associate on behalf of CCHCS, that imposes the same restrictions and conditions on such agents, subcontractors and vendors that apply to Business Associate with respect to such PHI and PII under this Agreement 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 PII. 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 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 Agreement into each subcontract or sub award to such agents, subcontractors and vendors, including the requirement that any security incidents or breaches of unsecured PHI or PII 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:
            1. Provide an opportunity for the subcontractor to cure the breach or end the violation and terminate the agreement if the subcontractor does not cure or end the violation within the time specified by CCHCS; or
            2. Immediately terminate the agreement if the subcontractor has breached a material term of the agreement and cure is not possible.
      6. Availability of Information to CCHCS and Individuals. To provide access and information:
         1. CCHCS may require Business Associate to deliver to CCHCS (or as directed by CCHCS to another individual or entity) PHI in a Designated Record Set upon reasonable notice in the time and manner designated by CCHCS and during Business Associate’s normal business hours in accordance with 45 CFR section 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 request 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.
         2. If Business Associate maintains an Electronic Health Record with PHI and a copy of such information is requested in an electronic format, Business Associate shall provide such information in an electronic format to enable CCHCS 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 CCHCS that was provided to CCHCS by the Social Security Administration, upon request by CCHCS Business Associate shall provide CCHCS 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.
      7. Amendment of PHI. To make any amendment(s) to PHI that CCHCS directs or agrees to pursuant to 45 CFR section 165.526, in the time and manner designated by CCHCS.
      8. Internal Practices. To make Business Associate’s internal practices, books and records available to CCHCS or to the Secretary of the U.S. Department of Health and Human Services relating to the use and disclosure of PHI received from CCHCS, or created or received by Business Associate on behalf of CCHCS in a time and manner designated by CCHCS or by the Secretary for purposes of determining CCHCS compliance with the HIPAA 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 fails or refuses to furnish the information to Business Associate, Business Associate shall so certify to CCHCS and shall set forth the efforts it made to obtain the information.
      9. Documentation of Unauthorized Disclosures. To document and make available to CCHCS or at the direction of CCHCS such unauthorized disclosures of PHI within 14 calendar days of the request in the form and manner requested by CCHCS, 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).
      10. 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. Notice to CCHCS.
             1. To notify CCHCS immediately upon the discovery of a suspected security incident that involves data subject to this Business Associates Agreement. This notification will be by telephone call plus email or fax upon the discovery of the breach.
             2. To notify CCHCS within 24 hours by email or fax of the discovery of unsecured PHI or PII in electronic media or in any other media if the PHI or PII was, or is reasonably believed to have been accessed or acquired by an unauthorized person, any suspected security incident, intrusion or unauthorized access, use or disclosure of PHI or PII in violation of this Agreement and this Agreement, or potential loss of confidential data affecting this Agreement. A breach shall be treated as discovered by Business Associate as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of Business Associate.
             3. Notice shall be provided to the CCHCS Program 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, notice shall be provided by calling the CCHCS ITSD Service Desk immediately. Notice shall be made using the “CCHCS Information Security Incident Report” form (ISIR), attached hereto as Attachment 1 to this Agreement, including all information known at the time, and emailed to the CCHCS Information Security Office at [CCHCS-ISO@cdcr.ca.gov](mailto:CCHCS-ISO@cdcr.ca.gov).
             4. Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of PHI or PII, Business Associate shall take:

Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and

Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

* + - 1. Investigation and Investigation Report.
         1. Investigation. To immediately investigate such security incident, breach, or unauthorized access, use or disclosure of PHI or PII and the ISIR did not include all the requested information, then within 72 hours of the discovery, Business Associate shall submit an updated CCHCS Information Security Incident Report (ISIR) containing the information marked with an asterisk and all other applicable information listed on the ISIR known at the time, to the CCHCS Program Contract Manager, the CCHCS Privacy Officer, and the CCHCS Information Security Officer.
         2. Complete Report. To provide a complete report of the investigation to the CCHCS Program Contract Manager, the CCHCS Privacy Officer, and the CCHCS information Security Officer within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. If all the required information was not included in either the initial report or the Investigation Report, then a separate Complete Report must be submitted. The report shall be submitted on the CCHCS Information Security Incident Report form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable provisions of HIPAA, the HITECH Act, the HIPAA regulations and/or state law. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If CCHCS request information in addition to that listed on the CCHCS Information Security Incident Report form, Business Associate shall make reasonable efforts to provide CCHCS with such information. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated “CCHCS Information Security Incident Report” form. CCHCS will review and approve or disapprove the determination of whether a breach occurred, is reportable to the appropriate entities, if individual notifications are required, and the corrective action plan.
         3. De-identification of Individuals. If the cause of a breach of PHI or PII is attributable to Business Associate or its subcontractors, agents or vendors, Business Associate shall notify individuals of the breach or unauthorized use disclosure when notification is required under state or federal law and shall pay any costs of such notifications, as well as any cost associated with the breach. The notifications shall comply with requirements set forth in 42 O.S.C. section 17932 and 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 CCHCS Program Contract Manager, the CCHCS Privacy Officer, and the CCHCS 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.
      2. Responsibility for Reporting of Breaches. If the cause of a breach PHI or PII 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 notifications 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 and Business Associate has reason to believe that duplicate reporting of the same breach or incident to CCHCS in addition to Business Associate may occur, Business Associate shall notify CCHCS, and CCHCS and Business Associate may take appropriate action to prevent duplicate reporting. The breach reporting requirements of this paragraph are in addition to the reporting requirements set forth in above subsections a and b of this section, Breaches and Security Incidents.
      3. 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 or the Agreement to which it is incorporated.

| **CCHCS Program Contract Manager** | **CCHCS Privacy Officer** | **CCHCS Information Security Officer** |
| --- | --- | --- |
| 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](mailto:Privacy@cdcr.ca.gov)  Telephone: 1-877-974-4722 | Information Security Officer  CCHCS Information Technology Services Division  P.O. Box 588500,  Bldg., C3  Elk Grove, CA 95758  Email: [CCHCS-ISO@cdcr.ca.gov](mailto:CCHCS-ISO@cdcr.ca.gov)  Fax: 916-691-3442  Telephone:916-691-3243 |

* + 1. Training Requirement. In accordance with CCHCS policy, all personnel assigned by the Contractor or any of its subcontractors pursuant to the underlying Agreement who access CCHCS systems shall complete Privacy Awareness and Information Security Awareness Training that is required of all individuals who may access PHI or PII before being provided credentials to access such information.
    2. Termination of Agreement.In accordance with Section 13404 (b) of the HITECH Act and to the extent required by the HIPAA regulations, if Business Associate knows of a material breach or violation by CCHCS if this Agreement, the Business Associates shall take the following steps:
       1. Provide an opportunity for CCHCS to cure the breach or end the violation and terminate the Agreement if CCHCS does not cure the breach or end the violation within the time specified by Business Associate; or
       2. Immediately terminate the Agreement if CCHCS has breached a material term of the Agreement and cure is not possible.
    3. Due Diligence. Business Associate shall exercise and shall take reasonable steps to ensure that it remains in compliance with this Agreement 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 Agreement.
    4. Sanctions and/or Penalties. Business Associates understands that a failure to comply with the provisions of HIPAA, the HITECH Act, and the HIPAA regulations that are applicable to Business Associates may result in the imposition of sanctions and/or penalties on Business Associate under HIPAA the HITECH Act and the HIPAA regulations.

1. **OBLIGATIONS OF CCHCS**
   1. CCHCS agrees:
      1. Notice of Privacy Practices. To provide Business Associate with the Notice of Privacy Practices that CCHCS produces in accordance with 45 CFR section 164.520, as well as any changes to such notice. The most current CCHCS Notice of Privacy Practices is attached to this Agreement as Attachment 2 to this Agreement.
      2. Permission by Individuals for Use and Disclosure of PHI. To 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.
      3. Notification of Restrictions. To notify the Business Associate of any restriction to the use or disclosure of PHI that CCHCS has agreed to in accordance with 45 CFR section 164.522, to the extent that such restriction may affect the Business Associate’s use or disclosure of PHI.
      4. 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 if done by CCHCS.
2. **AUDITS, INSPECTIONS AND ENFORCEMENT**
   1. Inspection.From time to time, CCHCS may inspect the facilities, systems, books and records of Business Associate to monitor compliance with this Agreement. Business Associate shall promptly remedy any violation of any provisions of this Agreement and shall certify the same to the CCHCS Privacy Officer in writing. The fact that CCHCS 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 Agreement, nor does CCHCS’ failure to detect or failure to notify Business Associate or require Business Associate’s remediation of any unsatisfactory practices constitute acceptance of such practice or a waiver of CCHCS enforcement rights under this Agreement.
   2. Notification Requirement.If Business Associate is the subject of an audit, compliance review, or complaint investigation by the Secretary of 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 Agreement, Business Associate shall notify CCHCS and provide CCHCS with a copy of any PHI or PII that Business Associate provides to the Secretary or the Office of Civil Rights concurrently by providing such PHI or PII 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).
3. **TERMINATION**
   1. Term.The term of this HIPAA Business Associate Agreement shall commence as of the effective date of the Agreement to which it attaches and shall extend beyond the termination of the contract and shall terminate when all the PHI provided by CCHCS to Business Associate or created or received by Business Associate on behalf of CCHCS is destroyed or returned to CCHCS in accordance with 45 CFR 164.504(e) (2) (ii) (l).
   2. Termination for Cause. In accordance with 45 CFR section 164.504(e) (1) (ii), upon CCHCS knowledge of material breach or violation 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; or
      2. Immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible.
   3. 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 in any administrative or civil proceeding in which the Business Associate is a party or has been joined.
   4. 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. If return or destruction is not feasible, Business Associate shall notify CCHCS of the conditions that make the return or destruction infeasible, and CCHCS 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 Agreement 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.
4. **MISCELLANEOUS PROVISIONS**
   1. 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 and accountable for all decisions made by Business Associate or its subcontractors regarding the safeguarding of PHI.
   2. Carrying out of Covered Entity’s Obligations. To the extent the underlying Agreement to which this Business Associate Agreement is attached requires the Business Associate to carry out CCHCS obligations under the HIPAA Privacy Rule, Business Associate agrees to comply with all requirements applicable to that obligation in the performance of the Agreement under Subpart E of 45 CFR Part 164.
   3. 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 is necessary to implement the standards and requirements of HIPAA, the HITECH Act, the HIPAA regulations and other applicable state 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 embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, the HIPAA regulations or other applicable state laws. CCHCS may terminate this Agreement upon thirty (30) days written notice in the event:
      1. Business Associate fails to promptly enter into an amendment to this Agreement when requested by CCHCS pursuant to this Section; or
      2. Business Associate fails to enter into an amendment to this Agreement 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.
   4. 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 CCHS at no cost to CCHCS to testify as witnesses or otherwise in the event of litigation or administrative proceedings being commenced against CCHCS, 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.
   5. 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.
   6. Interpretation.The terms and conditions in this Agreement 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 Agreement shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act, and the HIPAA regulations.
   7. 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.
   8. Survival.The obligations of Business Associate under this Agreement shall survive the termination of the Agreement to which this HIPAA Business Associate Agreement attaches.
   9. 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.
5. **BUSINESS ASSOCIATE DATA SECURITY REQUIREMENTS**
   1. Personnel Controls
      1. Training.All workforce members, whether employees, independent contractors or subcontractors of Business Associate who assist in the performance of functions or activities on behalf of CCHCS, or access or disclose CCHCS PHI or PII on CCHCS systems 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. 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 or work assignment, whether by employment or contract where appropriate.
      3. Confidentiality Statement*.*All persons that will be working with CCHCS 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 CCHCS PHI or PII. The statement must be renewed annually. The Contractor shall retain each person’s written confidentiality statement for CCHCS inspection for a period of six (6) years following contract termination.
      4. Background Check.Before a member of the workforce may access CCHCS PHI or PII, a thorough background check of that workforce member must be conducted, 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.
   2. Technical Security Controls
      1. Workstation/Laptop encryption. All workstations and laptops that process and/or store CCHCS PHI or Pl must be encrypted using a FIPS 140-2 Annex A certified algorithm which is 256 bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the CCHCS Information Security Office.
      2. Server Security. Servers containing unencrypted CCHCS PHI or PII must have appropriate 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 CCHCS PHI or PII required to perform necessary business functions may be copied, downloaded, or exported.
      4. Removable media devices. Per NIST 800-53 controls, all electronic files that contain CCHCS PHI or PII 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 FlPS 140-2 Annex A listed certified algorithm such as AES, which is 256 bit or higher per CCHCS standards.
      5. Antivirus software. All workstations, laptops and other systems that process and/or store CCHCS PHI or PII 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 CCHCS 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.
      7. User IDs and Password Controls. All users must be issued a unique user name for accessing CCHCS PHI or PII. Usernames must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password within 24 hours. Passwords are not to be shared. Passwords must be at least eight characters and must be a non­dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every 90 days and 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)
      1. Data Destruction. When no longer needed, all CCHCS PHI or PII must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the PHI or Pl cannot be retrieved.
      2. System Timeout. The system providing access to CCHCS PHI or PII must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of non-activity.
      3. Warning Banners. All systems providing access to CCHCS 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.
      4. System Logging. The system must maintain an automated audit trail which can identify the user or system process which initiates a request for CCHCS PHI or PII, or which alters CCHCS 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 CCHCS PHI or PII is stored in a databal.se, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.
      5. Access Controls. The system providing access to CCHCS PHI or PII must use role-based access controls for all user authentications, enforcing the principle of least privilege.
      6. Transmission encryption. All data transmissions of CCHCS PHI or PII outside the secure internal network must be encrypted using a FlPS 140-2 certified algorithm which is 256 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.
      7. Intrusion Detection. All systems involved in accessing, holding, transporting, and protecting CCHCS PHI or PII that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.
   3. Audit Controls
      1. System Security Review.All systems processing and/or storing CCHCS 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.
      2. Log Reviews, Business Continuity, and Disaster Recovery Controls.All systems processing and/or storing CCHCS PHI or PII must have a routine procedure in place to review system logs for unauthorized access.
      3. Change Control.All systems processing and/or storing CCHCS PHI or PII must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.
   4. Business Continuity and 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 CCHCS 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.
      2. Data Backup Plan.Contractor must have established documented procedures to backup CCHCS PHI to maintain retrievable exact copies of CCHCS 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 CCHCS PHI or PII should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of CCHCS data.
   5. Paper Document Controls
      1. Supervision of Data. CCHCS 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. CCHCS 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.
      2. Escorting Visitors. Where applicable, visitors to areas where CCHCS PHI or PII is contained shall be escorted and CCHCS PHI or PII shall be kept out of sight while visitors are in the area.
      3. Confidential Destruction. CCHCS PHI or PII must be disposed of through confidential means, such as cross cut shredding and pulverizing
      4. Removal of Data. CCHCS PHI or PII must not be removed from the premises of the Contractor except with express written permission of CCHCS.
      5. Faxing. Faxes containing CCHCS 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.
      6. Mailing. Mailings of CCHCS 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 CCHCS 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 CCHCS to use another method is obtained.

X. EFFECTIVE DATE AND EXECUTION

1. This HIPAA Business Associate Agreement shall be agreed to and effective upon execution of the Agreement number to which it is attached as an Exhibit and is incorporated by reference thereto.

1. These definitions are set forth in the Code of Federal Regulations (CFR); Title 45, Public Welfare:   
   [PART 160—GENERAL ADMINISTRATIVE REQUIREMENTS](http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=baa4845e4c964826deb54d0b59009602&n=45y1.0.1.3.76&r=PART&ty=HTML) § 160.103 Definitions.

   [PART 162--ADMINISTRATIVE REQUIREMENTS](http://www.ecfr.gov/cgi/t/text/text-idx?c=ecfr&SID=baa4845e4c964826deb54d0b59009602&rgn=div5&view=text&node=45:1.0.1.3.77&idno=45) § 162.103 Definitions.

   [PART 164--SECURITY AND PRIVACY](http://www.ecfr.gov/cgi/t/text/text-idx?c=ecfr&SID=baa4845e4c964826deb54d0b59009602&rgn=div5&view=text&node=45:1.0.1.3.79&idno=45) § 164.103 Definitions.

   Revision date May 7, 2019, Ver. 5.0 [↑](#footnote-ref-1)