

# **ATTACHMENT E**



**EXHIBIT E**  
**CONFIDENTIALITY AND INFORMATION SECURITY PROVISIONS**

These Confidentiality and Information Security Provisions (for HIPAA/HITECH Act contracts) set forth the information privacy and security requirements Contractor is obligated to follow with respect to all confidential information (as defined herein) disclosed to Contractor, or collected, created, maintained, stored, transmitted, or used by Contractor for or on behalf of the California Department of State Hospitals (DSH), pursuant to Contractor's agreement with DSH. DSH and Contractor (the parties) desire to protect the privacy and provide for the security of DSH confidential information pursuant to this Exhibit and in compliance with state and federal laws applicable to the confidential information.

**1. CONFIDENTIALITY AND INFORMATION SECURITY PROVISIONS:**

- A. Contractor shall comply with applicable laws and regulations, including but not limited to Welfare and Institutions Code sections 14100.2 and 5328 et seq. (2021), the Lanterman-Petris-Short Act, Civil Code section 1798 et seq. (2021), the Information Practices Act of 1977, Health and Safety Code section 123100 et seq. (2021), the Patient Access to Health Records Act, Title 42, Code of Federal Regulations (C.F.R.) part 431.300 et seq. (2021), and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), including but not limited to section 1320d et seq. of Title 42 of the United States Code and its implementing regulations (including but not limited to Title 45, Code of Federal Regulations (C.F.R.), parts 160, 162 and 164 (2021) (HIPAA regulations) regarding the confidentiality and security of protected health information (PHI). The following provisions of this Exhibit set forth some of the requirements of these statutes and regulations. This Exhibit should not be considered an exclusive list of the requirements. Contractor is required to fulfill the requirements of these statutes and regulations by independently researching and obtaining legal advice on these requirements as they may be amended from time to time.
- B. Order of Precedence: With respect to confidentiality and information security provisions for all DSH confidential information, the terms and conditions of this Exhibit shall take precedence over any conflicting terms or conditions set forth in any other part of the agreement between Contractor and DSH, including Exhibit A (Scope of Work), all other exhibits and any other attachments, and shall prevail over any such conflicting terms or conditions.
- C. Effect on lower tier transactions: The terms of this Exhibit shall apply to all contracts, subcontracts, and subawards, and the information privacy and security requirements Contractor is obligated to follow with respect to DSH confidential information disclosed to Contractor, or collected, created, maintained, stored, transmitted or used by Contractor for or on behalf of DSH, pursuant to Contractor's agreement with DSH. When applicable, the Contractor shall incorporate the relevant provisions of this Exhibit into each subcontract or subaward to its agents, subcontractors, or independent consultants.

**2. DEFINITIONS:**

- A. The following terms used in the agreement between DSH and Contractor shall have the same meaning as those terms in the HIPAA Rules: Breach, Covered Entity, Data Aggregation, Disclosure, Health Care Operations, Individual, Minimum Necessary, Protected Health Information, Secretary, Subcontractor, Unsecured Protected Health Information, and Use.
- B. Specific Definitions
  - i. Contractor. Contractor shall have the same meaning as the term "business associate" at 45 C.F.R. section 160.103 (2021).

- ii. Breach. With respect to Contractor's handling of confidential information, "breach" shall have the same meaning as the term "breach" in HIPAA, 45 C.F.R. section 164.402 (2021).
- iii. HIPAA Rules. HIPAA Rules shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. parts 160 and 164 (2021).
- iv. Confidential Information. Confidential information shall mean information or data that is Protected Health Information or Personal Information as defined herein.
- v. Personal Information (PI). Personal Information shall have the same meaning as defined in Civil Code section 1798.3, subdivision (a) (2021).
- vi. Required by law, as set forth under 45 C.F.R. section 164.103 (2021), shall mean 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.
- vii. Security Incident. Security Incident shall mean the intentional 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 Contractor's organization and intended for internal use; or interference with system operations in an information system.

### **3. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE:**

#### **A. Contractor agrees to:**

- i. not use or disclose confidential information other than as permitted or required by the agreement between DSH and Contractor or as required by law. Any use or disclosure of DSH confidential information shall be the Minimum Necessary;
- ii. use appropriate safeguards, and comply with Subpart C of 45 C.F.R. part 164 (2021) with respect to electronic confidential information, to prevent use or disclosure of confidential information other than as provided for by the agreement with DSH;
- iii. report to DSH any use or disclosure of confidential information not provided for by the agreement with DSH of which it becomes aware, including breaches of unsecured protected health information as required at 45 C.F.R. section 164.410 (2021), and any security incident of which it becomes aware;
- iv. in accordance with 45 C.F.R. sections 164.502(e)(1)(ii) and 164.308(b)(2) (2021), if applicable, ensure that any agents and subcontractors that create, receive, maintain, or transmit confidential information on behalf of Contractor enter into a written agreement with Contractor agreeing to be bound to the same restrictions, conditions, and requirements that apply to Contractor with respect to such information;
- v. to provide access and make available confidential information in a designated record set to DSH or to an Individual in accordance with 45 C.F.R. section 164.524 (2021) and

California Health and Safety Code section 123100 et seq. (2021). Designated Record Set shall mean the group of records maintained for DSH that includes medical, dental, and billing records about individuals; enrollment, payment, claims adjudication, and case or medical management systems maintained for DSH health plans; or those records used to make decisions about individuals on behalf of DSH. Contractor shall use the forms and processes developed by DSH for this purpose and shall respond to requests for access to records transmitted by DSH within fifteen (15) calendar days of receipt of the request by producing the records or verifying that there are none;

- vi. if Contractor maintains an Electronic Health Record with PHI and an Individual requests a copy of such information in an electronic format, Contractor shall provide such information in an electronic format to enable DSH to fulfill its obligations under the HITECH Act, including but not limited to, 42 U.S.C. section 17935(e) (2021);
- vii. if Contractor receives data from DSH that was provided to DSH by the Social Security Administration, upon request by DSH, Contractor shall provide DSH with a list of all employees, subcontractors, and agents who have access to the Social Security data, including employees, contractors, and agents of its subcontractors and agents;
- viii. make any amendment(s) to confidential information in a Designated Record Set as directed or agreed to by DSH pursuant to 45 C.F.R. section 164.526 (2021), or take other measures as necessary to satisfy DSH's obligations under 45 C.F.R. section 164.526 (2021);
- ix. to document and make available to DSH or (at the direction of DSH) to an Individual within 15 days such disclosures of PHI, and information related to such disclosures, necessary to respond to a proper request by the Individual for an accounting of disclosures of PHI, in accordance with the HITECH Act and its implementing regulations, including but not limited to 45 C.F.R. section 164.528 (2021) and 42 U.S.C. section 17935(c) (2021). If Contractor maintains electronic health records for DSH as of January 1, 2009, Contractor 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 Contractor acquires electronic health records for DSH after January 1, 2009, Contractor 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;
- x. to the extent Contractor is to carry out one or more of DSH's obligation(s) under Subpart E of 45 C.F.R. part 164 (2021), comply with the requirements of Subpart E that apply to DSH in the performance of such obligation(s); and
- xi. make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA regulations.
- xii. comply with all legal obligations pursuant to the California Consumer Privacy Protection Act (CCPA) of Contractor, its employees, agents and sub-contractors, including but not limited to the handling and disclosure of personal information received resulting from this agreement, abiding by CCPA notice requirements on Contractor's website(s), safeguarding personal information received in connection with this agreement, refraining from using personal information received in connection with this agreement outside of the enumerated business purpose contained therein. Contractor's failure to comply with such

laws and regulations shall constitute a material breach of this Agreement, and shall be grounds for immediate termination of the Agreement by DSH, pursuant to section 7 of Exhibit C. By executing this Agreement, Contractor certifies that it is aware of its legal obligations as set forth under the CCPA, that it is in compliance with the CCPA, and shall remain in compliance with all such laws and regulations for the term of this Agreement.

xiii. indemnify and hold the DSH harmless from and against any and all liability, loss, suit, damage or claim, including third party claims brought against the DSH, pursuant to section 5 of Exhibit C of this Agreement, as well as damages and reasonable costs assessed against the DSH by a court of competent jurisdiction (or, at Contractor's option, that are included in a settlement of such claim or action in accordance herewith), to the fullest extent permitted by State law, to the extent such claim arises from Contractor's violation of the CCPA in relation to Contractor's performance under this agreement; provided, that (i) Contractor is notified promptly in writing of the claim; (ii) Contractor controls the defense and settlement of the claim; (iii) Contractor provides a defense with counsel approved by the DSH; and (iv) the DSH cooperates with all reasonable requests of Contractor (at Contractor's expense) in defending or settling the claim.

#### **4. PERMITTED USES AND DISCLOSURES OF CONFIDENTIAL INFORMATION BY THE CONTRACTOR:**

- A. Except as otherwise provided in the agreement between Contractor and DSH, Contractor, may use or disclose DSH confidential information to perform functions, activities or services identified in the agreement with DSH provided that such use or disclosure would not violate federal or state laws or regulations.
- B. Contractor may not use or disclose the confidential information except as provided and permitted or required by this agreement with DSH or as required by law.
- C. Contractor may use and disclose confidential information for the proper management and administration of the Contractor or to carry out the legal responsibilities of the Contractor, provided that such uses and disclosures are required by law.
- D. Contractor may use confidential information to provide data aggregation services related to the health care operations of the DSH. Data aggregation means the combining of DSH confidential information created or received by Contractor on behalf of DSH with confidential information received by Contractor in its capacity as the business associate of another Covered Entity, to permit data analyses that relate to the health care operations of DSH.

#### **5. SAFEGUARDS:**

- A. Contractor shall develop and maintain an information privacy and security program that includes the implementation of administrative, technical, and physical safeguards. The information privacy and security program shall reasonably and appropriately protect the confidentiality, integrity, and availability of the confidential information that it creates, receives, maintains, or transmits; and prevent the use or disclosure of confidential information other than as provided for by the agreement with DSH. Contractor shall provide the DSH with information concerning such safeguards as the DSH may reasonably request from time to time.
- B. Contractor shall implement administrative, technical, and physical safeguards to ensure the security of the DSH information on portable electronic media (e.g., USB drives and CD-ROM) and in paper files. Administrative safeguards to be implemented shall include, but are not limited to training, instructions to employees, and policies and procedures regarding the HIPAA Privacy

Rule. Technical safeguards to be implemented must comply with the HIPAA Security Rule and Subpart C of part 164 of the HIPAA regulations with respect to electronic confidential information, and shall include, but are not limited to, role-based access, computer passwords, timing out of screens, storing laptop computers in a secure location (never leaving the equipment unattended at workplace, home or in a vehicle) and encryption. Physical safeguards to be implemented shall include, but are not limited to, locks on file cabinets, door locks, partitions, shredders, and confidential destruct.

## 6. AUTHENTICATION:

- A. Contractor shall implement appropriate authentication methods to ensure information system access to confidential information is only granted to properly authenticated and authorized persons. If passwords are used in user authentication (e.g., username/password combination), Contractor shall implement strong password controls on all compatible computing systems that are consistent with the National Institute of Standards and Technology (NIST) Special Publication 800-53 and the SANS Institute Password Protection Policy.
- i. Contractor shall implement the following security controls on each server, workstation, or portable (e.g., laptop computer) computing device that processes or stores confidential, personal, or sensitive data:
- (1) network-based firewall and/or personal firewall,
  - (2) continuously updated anti-virus software and
  - (3) patch-management process including installation of all operating system/software vendor security patches.
- ii. Encrypt all confidential, personal, or sensitive data stored on portable electronic media (including, but not limited to, CDs and thumb drives) and on portable computing devices (including, but not limited to, laptop computers, smart phones and PDAs) with a solution that uses proven industry standard algorithms.
- iii. Prior to disposal, sanitize all DSH confidential data contained in hard drives, memory devices, portable electronic storage devices, mobile computing devices, and networking equipment in a manner consistent with the National Institute of Standards and Technology (NIST) Special Publication 800-88.
- iv. Contractor shall not transmit confidential, personal, or sensitive data via e-mail or other Internet transport protocol over a public network unless, at minimum, a 128-bit encryption method (for example AES, 3DES, or RC4) is used to secure the data.

## 7. MITIGATION OF HARMFUL EFFECTS:

- A. Contractor shall mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of confidential information by Contractor or its subcontractors in violation of the requirements of the agreement.

## 8. NOTIFICATION OF BREACH:

- A. During the term of the agreement with DSH, Contractor shall report to DSH any use or disclosure of information not provided for by its contract of which it became aware including breaches of unsecured confidential information as required by 45 C.F.R. section 164.410 (2021).

**9. DISCOVERY OF BREACH:**

- A. Contractor shall immediately notify the DSH Chief Information Security Officer by telephone call and email upon the discovery of a breach of confidential information in all forms (paper, electronic, or oral) if the confidential information was, or is reasonably believed to have been, acquired by an unauthorized person, or within 24 hours by email or fax of the discovery of any suspected security incident, intrusion or unauthorized use or disclosure of confidential information in violation of the agreement with DSH, or potential loss of DSH confidential data. If the security incident occurs after business hours or on a weekend or holiday, notification shall be provided by calling the DSH Chief Information Security Officer. Contractor shall take:
  - i. prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and
  - ii. any action pertaining to such unauthorized disclosure required by applicable federal and state laws and regulations.

**10. INVESTIGATION OF BREACH:**

- A. Contractor shall immediately investigate such security incident, breach, or unauthorized use or disclosure of DSH confidential information. Within 8 hours of discovery (of the breach), Contractor shall notify the DSH Chief Information Security Officer of at least the following:
  - i. the data elements involved and the extent of the confidential data involved in the breach;
  - ii. a description of the unauthorized person(s) known or reasonably believed to have improperly acquired, accessed, used, transmitted, sent or disclosed confidential information;
  - iii. a description of where and when the confidential information is believed to have been improperly acquired, accessed, used, transmitted, sent or disclosed;
  - iv. a description of the probable causes of the improper acquisition, access, use, transmission, sending, or disclosure; and
  - v. whether Civil Code sections 1798.29 or 1798.82 or any other federal or state laws requiring individual notifications of breaches are required.

**11. WRITTEN REPORT:**

- A. Contractor shall provide a written report of the investigation to the DSH Information Security Officer within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall include, but not be limited to, the information specified above, an estimation of cost for remediation, 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.

**12. NOTIFICATION OF INDIVIDUALS:**

- A. Contractor shall notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal law and to pay any costs of such notifications, as well as any costs associated with the breach. Notification shall be made in the most expedient time possible without reasonable delay. The DSH Program Contract Manager, DSH Chief Information Security Officer, and DSH Chief Privacy Officer shall approve the time, manner, and



content of any such notifications and their review and approval must be obtained by Contractor before the notifications are made.

**13. DSH CONTACT INFORMATION:**

- A. Contractor shall direct communications to the DSH Program Contract Manager, DSH Chief Information Security Officer, and DSH Chief Privacy Officer Contractor shall initiate contact as indicated herein. DSH reserves the right to make changes to the contact information below by giving written notice to Contractor. Said changes shall not require an amendment to the agreement between the parties to which it is incorporated.

DSH Contract Manager	DSH Chief Privacy Officer	DSH Chief Information Security Officer
See Exhibit A - Scope of Work for contact information	Chief Privacy Officer Office of Legal Services 1215 O Street, MS-5 Sacramento, CA 95814  Email: <a href="mailto:DSHSacLegalPrivacy@dsh.ca.gov">mailto:DSHSacLegalPrivacy@dsh.ca.gov</a> Telephone: 916-562-3721	Chief Information Security Officer Information Security Office 1215 O Street, MS-4 Sacramento, CA 95814  Email: <a href="mailto:iso@dsh.ca.gov">iso@dsh.ca.gov</a> and <a href="mailto:security@dsh.ca.gov">security@dsh.ca.gov</a> Telephone: 916-654-4218

**14. INTERNAL PRACTICES:**

- A. Contractor shall make Contractor's internal practices, books and records relating to the use and disclosure of DSH confidential information received from DSH, or created, maintained or received by Contractor, available to DSH or to the Secretary in a time and manner designated by DSH or by the Secretary, for purposes of determining DSH's compliance with HIPAA regulations.

**15. EMPLOYEE TRAINING AND DISCIPLINE:**

- A. Contractor shall train and use reasonable measures to ensure compliance with the requirements of the agreement between DSH and Contractor by employees who assist in the performance of functions or activities under this agreement and use or disclose confidential information; and discipline such employees who intentionally violate any provisions of this agreement.

**16. EFFECT OF TERMINATION:**

- A. Upon termination or expiration of the agreement between Contractor and DSH for any reason, Contractor shall return, at its sole expense, to DSH all confidential information within five (5) business days or as otherwise specified in the request or notice to return records or, if agreed to by DSH, destroy all confidential information received from DSH or created or received by Contractor on behalf of DSH, that Contractor still maintains in any form. Contractor shall retain no copies of DSH confidential information. However, if return or destruction is not feasible, Contractor shall continue to extend the protections and provisions of the agreement to such information, and limit further use or disclosure of such confidential information to those purposes that make the return or destruction of such confidential information infeasible. This provision shall apply to DSH confidential information that is in the possession of Contractor, its subcontractor(s), or its agent(s).

**17. MISCELLANEOUS PROVISIONS:**

- B. DSH shall notify Contractor and Contractor shall notify DSH of restrictions on disclosures or the manner of confidential communications requested and agreed to by Contractor or DSH from an Individual to satisfy 45 C.F.R. section 164.522 (2021).
- C. Assistance in Litigation or Administrative Proceedings. Contractor shall make itself, and use its best efforts to make any subcontractors, employees or agents assisting Contractor in the performance of its obligations under the agreement with DSH, available to DSH at no cost to DSH to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against DSH, its directors, officers or employees for claimed violations of HIPAA, regulations or other laws relating to security and privacy based upon actions or inactions of Contractor and/or its subcontractors, employees, or agents, except where Contractor or its subcontractors, employees, or agents is a named adverse party.
- D. No Third-Party Beneficiaries. Nothing expressed or implied in the terms and conditions of the agreement between Contractor and DSH is intended to confer, nor shall anything herein confer, upon any person other than DSH or Contractor and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.
- E. The terms and conditions in this Agreement shall be interpreted as broadly as necessary to implement and comply with the HIPAA regulations and applicable federal and state laws. The parties agree that any ambiguity in the terms and conditions of the agreement between the parties shall be resolved in favor of a meaning that complies and is consistent with state and federal law, including HIPAA and the HIPAA regulations.
- F. A reference in the terms and conditions of the agreement between DSH and Contractor to any HIPAA regulation relates to that section in effect or as amended.
- G. The obligations of Contractor under this Exhibit E shall survive the termination or expiration of the agreement.

**18. JUDICIAL OR ADMINISTRATIVE PROCEEDINGS:**

- A. DSH may immediately terminate the agreement between Contractor and DSH if (a) Contractor is found liable in a civil or criminal proceeding for a violation of the HIPAA Privacy or Security Rule or (b) a finding or stipulation that Contractor has violated a privacy or security standard or requirement of HIPAA, or other security or privacy laws made in an administrative or civil proceeding in which Contractor is a party.

**19. TERMINATION FOR CAUSE:**

- A. In accordance with 45 C.F.R. section 164.504(e)(1)(ii) (2021), upon DSH's knowledge of a material breach or violation of this Exhibit by Contractor, DSH shall:
  - i. Provide an opportunity for Contractor to cure the breach or end the violation and terminate the agreement if Contractor does not cure the breach or end the violation within the time specified by DSH; or
  - ii. Immediately terminate the agreement pursuant to section 7 of Exhibit C of this Agreement, if Contractor has breached a material term of this Exhibit and cure is not possible.