# HIPAA BUSINESS ASSOCIATE AGREEMENT

# ****Between The California Department of Technology (CDT)****

# ****and****

# ****<Department> (<Department Acronym>)****

Note: This template is for no-view hosting services provided directly by CDT, or by CDT through their contractors and business associates.

This Business Associate Agreement (BAA) is effective on \_\_\_\_\_\_\_\_\_\_\_\_, 20\_\_\_\_\_\_ (Effective Date), between the <Department> (<Department Acronym>) and the California Department of Technology (CDT) regarding CDT’s obligations as a Business Associate of <Department Acronym> for purposes of performing functions, activities or services in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH). <Department Acronym> and CDT are referred to collectively as “Parties” and individually as “Party.”

## RECITALS

<Department Acronym> is a <Covered Entity or Business Associate> as such term is defined under HIPAA. <Department Acronym> and CDT have entered into an Agreement, whereby CDT will provide certain functions, activities, or services for or to <Department Acronym>, and in the continued performance of these Services may receive, maintain, retain, store, or otherwise hold, Protected Health Information (PHI) from or on behalf of <Department Acronym>.

This BAA is intended to ensure that CDT will establish and implement appropriate safeguards, including certain physical, administrative, and technical security requirements to protect the <Department Acronym’s> PHI and to ensure that all of CDT’s agents, contractors, and Subcontractors shall also comply with the terms of this BAA.

### DEFINITIONS

The following terms used in this BAA shall have the same meaning as those terms in the HIPAA Rules: Breach, Business Associate, Covered Entity, Disclose or Disclosure, Individual, Protected Health Information, Required by Law, Security, Security Incident, Subcontractor, Unsecured PHI, and Use. Terms used but not otherwise defined in this BAA shall have the same meaning as those terms in the HIPAA Rules.

The following terms are defined below:

Agreement. “Agreement” means a contract, understanding, or relationship, whether documented in writing or not, between CDT and <Department Acronym> that is the basis for CDT’s Business Associate status.

Hosting Service Provider. “Hosting Service Provider” or “HSP” means an information technology (IT) service company or partner that provides remote IT resources and/or services enabling individuals, companies or [managed service providers (MSPs)](https://www.acronis.com/solutions/cloud/) to host websites, databases, applications and other critical systems.

HIPAA Rules. “HIPAA Rules” means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Parts 160, 162, and 164.

Privacy Rule. “Privacy Rule” means the standards of privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, Subparts A and E, respectively, as amended from time to time.

Security Rule. “Security Rule” means those provisions found in 45 C.F.R. Part 164, Subpart C, as amended from time to time.

Services. “Services” means the functions, activities, work, or assistance that CDT provides to <Department Acronym> and through which CDT, or its agents, contractors, or Subcontractors, may receive, maintain, retain, record, store, or otherwise hold PHI from or on behalf of <Department Acronym>.

### OBLIGATIONS AND ACTIVITIES OF CDT

1. CDT shall comply with all applicable requirements of HIPAA including, but not limited to, the HIPAA Rules, HIPAA regulations, the requirements of HITECH, and as may be updated from time to time. CDT shall comply with all relevant policies and procedures of the Statewide Health Information Policy Manual (SHIPM), the State Administrative Manual (SAM) Chapter 5300, and the State Information Management Manual (SIMM).
2. CDT, or its agents, contractors, Subcontractors, or Business Associates, shall not Use or Disclose PHI other than as permitted or required by the Agreement and this BAA or as Required by Law. If CDT performs the Services Not Permitted in Section II.B(ii) below, it might be a Breach.
3. Permitted Services: CDT may receive, maintain, retain, record, store, or otherwise hold PHI. CDT may transmit <Department Acronym’s> data, including PHI, to <Department Acronym’s> subscribed service provider or other entity either to perform Services in the Agreement, upon written request of <Department Acronym>, or when required by law.
	1. In the event of a Breach and upon written permission from <Department Acronym>, CDT may have access to and use PHI to the extent authorized.
4. Services Not Permitted: Except as otherwise permitted under the terms of the Agreement or this BAA, CDT may not create, modify, destroy, Use, Disclose, or have access to PHI. Regarding the destruction of PHI, CDT may not destroy PHI while this BAA is in effect. CDT may not transmit PHI unless transmission is authorized by Section II.B(i) above. If this BAA is terminated, CDT shall comply with Section IV below regarding destruction of <Department Acronym’s> PHI.
5. CDT shall periodically distribute the latest BAA template to all units that provide or may provide Services to the <Department Acronym’s> to ensure the correct template is being used, including CDT’s Subcontractors and Business Associates.
6. In the performance of the Services, CDT shall implement, maintain, and use appropriate safeguards, including administrative safeguards, physical safeguards, and technical safeguards, that:
7. protect the confidentiality, integrity, and availability of PHI as required by the HIPAA Rules;
8. comply with Subpart C of 45 C.F.R. Part 164 with respect to electronic PHI; and
9. implement, if applicable, any other <Department Acronym’s> requirements necessary for compliance with applicable federal and state law, as set forth in the separately negotiated and executed Attachment [X], attached hereto.
10. CDT shall prevent Use or Disclosure of PHI other than as provided for by the Agreement and this BAA or as Required by Law. CDT’s safeguards shall include, without limitation,
11. implementing written policies and procedures in compliance with HIPAA, the HIPAA Rules, HITECH, and the SHIPM;
12. conducting a security risk assessment;
13. conducting risk assessments concerning possible Breaches; and
14. providing annual HIPAA privacy and security awareness training to its employees and other workforce.
15. As CDT will not access <Department Acronym’s> data to know the location of PHI in CDT’s system, any Breach of <Department Acronym’s> data of any kind shall be considered a Breach of PHI, unless CDT has evidence that the data is not PHI. Because CDT will not access <Department Acronym’s> data, CDT shall treat all <Department Acronym’s> data as if it is PHI, subject to the HIPAA rules and this BAA.
16. CDT shall notify Cal-CSIRS as soon as practicable of any Breach of data related to <Department Acronym> that it identifies in CDT’s systems.
17. CDT shall report to <Department Acronym> any access, Use, or Disclosure of PHI that is not provided for by the Agreement and this BAA, including Breaches of Unsecured PHI as required by 45 C.F.R. part 164.410; and shall report to <Department Acronym> any Security Incident of which CDT becomes aware. All such reports and notices shall be sent in writing within 24 hours of the suspected Breach or Security Incident to the <Department Acronym’s> [Information Security Officer at: @XXX.ca.gov].
18. CDT shall, as reasonably necessary, cooperate with and assist <Department Acronym> in any Breach investigation. CDT may have access to PHI as noted above in Section II.B(i)(a) to the extent authorized and shall protect such PHI consistent with this BAA.
19. In the event of a Breach, CDT will provide as much information as is available and knowable at the given point in the investigation, as follows:
20. the identification of each Individual whose PHI has been, or is reasonably believed by CDT to have been accessed, acquired, created, modified, transmitted, destroyed, or Disclosed during such Breach;
21. a brief description of what happened, including the date of the Breach and discovery of the Breach;
22. a description of the type of PHI that was involved in the Breach;
23. a description of the investigation into and risk assessment concerning the Breach, mitigation of harm to the Individual(s), and protection against further Breaches;
24. the results of any and all investigations and risk assessments performed by CDT related to the Breach; and
25. contact information of the most knowledgeable individual within CDT for <Department Acronym> to contact relating to the Breach and its investigation into and risk assessment concerning the Breach.
26. CDT shall bear all financial costs associated with a Breach arising out of or relating to the breach of its obligations under the Agreement and this BAA by CDT, except to the extent such Breach is due to the negligence or willful misconduct of <Department Acronym>.
27. CDT shall take all reasonable steps to mitigate any harmful effect that is known to it of a Use or Disclosure of PHI by CDT in violation of the Agreement and this BAA or of any Security Incident of which it becomes aware.
28. In the event of a breach, to the extent that CDT has or has access to relevant information, CDT shall cooperate and assist <Department Acronym> in meeting all legally mandated reporting requirements.
29. CDT shall ensure that its agents, contractors, Subcontractors, or Business Associates that receive, maintain, retain, record, store, transmit, or otherwise hold PHI in connection with the Services agrees and provide written assurances in compliance with the HIPAA Rules to the same restrictions, conditions, and requirements that apply through this BAA to CDT with respect to <Department Acronym’s> data, including PHI.
30. CDT shall make its employees and agents available to <Department Acronym> at no cost to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings against <Department Acronym>, its directors, officers, and/or employees based on claimed violations of HIPAA that involve actions or inactions by CDT.
31. If CDT is the subject of an audit, compliance review, investigation or any proceeding that is related to the performance of its obligations under this BAA or is otherwise the subject of any judicial or administrative proceeding alleging a violation of HIPAA, CDT shall promptly notify <Department Acronym> unless it is legally prohibited from doing so.
32. CDT represents that it is a no-view Hosting Service Provider (HSP) as defined in this BAA agreement. As a no-view entity, CDT represents that it lacks access to the decryption key(s) to see or decode <Department Acronym’s> PHI stored in its servers.
33. CDT shall provide any relevant information in CDT’s possession to assist <Department Acronym> in its responsibility related to an accounting of disclosures within the necessary timeframe for <Department Acronym> to meet its statutory obligation.
34. CDT shall maintain the necessary confidentiality, integrity, and availability of the PHI for the benefit of <Department Acronym> at all times, so that the <Department Acronym> can meet all its Use and Disclosure needs and in order to meet the following requirements:
35. To ensure that CDT does not access, Use, or Disclose <Department Acronym’s> PHI, CDT will refer Individuals who request the following to <Department Acronym> within a timeframe that will ensure <Department Acronym> can comply with legal deadlines:
36. access to PHI,
37. an accounting of disclosures,
38. confidential communications, and
39. amendment of PHI.
40. CDT shall make its internal practices, books, and records, including policies and procedures relating to the Agreement and this BAA available to <Department Acronym> and/or to the Secretary (or its agents) of the federal Health and Human Services in a reasonable time and manner designated by <Department Acronym> or the Secretary.

### OBLIGATIONS OF <Department Acronym>

1. <Department Acronym> shall periodically review this BAA and make required updates to ensure this BAA is accurate and consistent with the law.
2. <Department Acronym> is responsible for making modifications to the data, including PHI, held by CDT.
3. Only <Department Acronym> is able to view the PHI maintained by CDT. <Department Acronym> shall ensure only the appropriate staff within <Department Acronym> access, Use, or Disclose <Department Acronym’s> PHI. Therefore, <Department Acronym> is responsible for certain access controls, such as authentication or unique user identification related to its own staff.
4. To ensure that CDT does not access <Department Acronym’s> PHI, <Department Acronym> is responsible for making the required Breach notifications to consumers and oversight entities as required by law and policy (see Section II.B above).

### IV. TERM AND TERMINATION

1. Term. This BAA shall be effective upon execution of this BAA. This BAA shall remain in effect as long as CDT is performing the Services in accordance with this BAA or until this BAA is terminated and all requirements of this Section IV are met regarding return or destruction of PHI.
2. Unless otherwise Required by Law, CDT shall destroy or return to <Department Acronym>, within thirty (30) days of the termination of the Agreement or this BAA, all PHI. Since CDT is not able to access, Use, or Disclose <Department Acronym’s> PHI, or to know what data is PHI, CDT shall destroy or return all <Department Acronym’s> data. Upon such destruction or return, CDT shall provide a written certification to <Department Acronym> within thirty (30) days of termination of this BAA that includes all of the following: (i) a statement confirming that all of the data, including PHI, has been destroyed or returned to <Department Acronym>; and (ii) a statement that describes the mechanism by which all of the data, including PHI, was destroyed or returned to the <Department Acronym>. This certification shall be provided to the <Department Acronym> Information Security Officer at @XXX.ca.gov.
3. In the event that CDT’s return or destruction of all or part of <Department Acronym’s> data, including PHI, is infeasible at the termination of the Agreement or this BAA, CDT shall notify <Department Acronym> and discuss a mutually agreed upon risk assessment with <Department Acronym’s> Privacy Officer or Information Security Officer of the reason(s) that makes such return or destruction infeasible and the duration for which the <Department Acronym’s> data must be retained. This will be the Retention Period. CDT shall continue to safeguard <Department Acronym’s> data under the terms and conditions set forth in the Agreement and this BAA for as long as CDT retains the data and shall return and or destroy such data when the Retention Period has expired.
4. Termination for Cause. Upon <Department Acronym’s> knowledge of a material breach of the Agreement, this BAA, HIPAA, the HIPAA Rules, HIPAA regulations and/or HITECH by CDT, <Department Acronym> shall either:
5. Provide an opportunity for CDT to cure the breach or end the violation, or terminate this BAA if CDT does not cure the breach or end the violation within the time specified by <Department Acronym>; or
6. Immediately terminate the Agreement and this BAA if CDT has breached a material term of the Agreement or this BAA and cure is not possible.

### MISCELLANEOUS

1. The Parties may negotiate additional terms related to protection, access, Use, and Disclosure of <Department Acronym's> data outside of this BAA.
2. The Parties agree to take such action as is necessary to amend this BAA from time to time as required for the Parties to comply with the provisions of HIPAA, the HIPAA Rules, HITECH, and any other applicable law or policies.
3. Any ambiguity in this BAA shall be interpreted and resolved to permit compliance with HIPAA, the HIPAA Rules, and HITECH.
4. In the event of an inconsistency between the terms of this BAA and the mandatory terms of the HIPAA Rules, the mandatory terms of the HIPAA Rules shall prevail. Where the terms of this BAA are different from those included in the HIPAA Rules but the terms of the HIPAA Rules are permissive, the terms of this BAA shall control. Similarly, in the event of an inconsistency between the terms of this BAA and the mandatory terms of state law, the mandatory terms of state law shall prevail. However, the terms of the HIPAA Rules shall control when the HIPAA Rules preempt state law.
5. This BAA shall be deemed to be amended upon any changes to the HIPAA Rules or state law impacting this BAA without the need for the Parties to re-sign or re-execute.
6. The Parties shall collaborate as appropriate and necessary to ensure compliance with this BAA. The Parties acknowledge and agree that neither Party intends that this BAA creates obligations and/or liabilities that do not otherwise exist as appropriate based on the nature of the work performed and applicable law.
7. Should any provision of this BAA be found unenforceable, it shall be deemed severed and the balance of the BAA shall continue in full force and effect as if the unenforceable provision had never been made a part hereof.
8. This BAA does not create or confer any rights or remedies onto third Parties.

**IN WITNESS WHEREOF**, the Parties have executed this BAA on the date indicated below.

California Department of Technology

By:

Printed Name:

Title:

Date:

<CA State Organization Name>

By:

Printed Name:

Title:

Date: