

BUSINESS ASSOCIATE AGREEMENT

WHEREAS, the San Jose Evergreen Community College District (“Covered Entity”) is a hybrid entity, performing both covered and non-covered functions under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), and seeks to disclose certain Protected Health Information (defined below) to Contractor (“Business Associate”) pursuant to the terms of the Agreement between the Parties to this Business Associate Agreement (BAA); and

WHEREAS, the Covered Entity and Business Associate intend to protect the privacy and provide for the security of PHI used and disclosed pursuant to this BAA in compliance with HIPAA; the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (the “HITECH Act”), and regulations promulgated thereunder by the U.S. Department of Health and Human Services (collectively, the “HIPAA Regulations”); California Confidentiality of Medical Information Act (Civil Code, §56 *et seq.*); California Health & Safety Code Section 1280.15 *et seq.*; and other applicable laws; and to the extent the Business Associate is to carry out the Covered Entity’s obligation under the Privacy Rule (defined below), the Business Associate must comply with the requirements of the Privacy Rule that apply to the Covered Entity in the performance of such obligation.

WHEREAS, part of the HIPAA Regulations, the Privacy Rule and the Security Rule (both of which are defined below) require covered entities to enter into a contract containing specific requirements with any business associate prior to the disclosure of PHI, as set forth in, but not limited to, Title 45, Sections 164.314(a), 164.502(e), and 164.504(e) of the Code of Federal Regulations (C.F.R.) and contained in this BAA.

NOW, THEREFORE, in consideration of the mutual promises below and the exchange of information pursuant to the BAA, the Parties agree as follows:

1. Definitions

Terms used, but not otherwise defined, and terms with initial capital letters in the BAA have the same meaning as defined under HIPAA, the HITECH Act, HIPAA Regulations, and other applicable laws.

- a. **Business Associate** is a person, organization, or agency other than a workforce member that provides specific functions, activities, or services that involve the use, creation, or disclosure of PHI for, or on behalf of, a HIPAA covered health care component. Examples of business associate functions are activities such as claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, practice management, repricing; and legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.
- b. **Designated Record Set** shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. §164.501.
- c. **Electronic Protected Health Information or ePHI** means Protected Health Information that is maintained in or transmitted by electronic media as defined by 45 C.F.R. § 160.103.
- d. **Electronic Health Record** shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C. Section 17921.
- e. **Health Care Operations** shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. §164.501.
- f. **Privacy Breach** shall mean any acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted or allowed under state or federal privacy laws.

- g. Privacy Rule** shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and E.
- h. Protected Health Information or PHI** means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present, or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (ii) 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, and shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. §160.103. Protected Health Information includes ePHI.
- i. Protected Information** shall mean PHI provided by Covered Entity to Business Associate or created or received by Business Associate on the Covered Entity's behalf.
- j. Security Incident** shall mean, as set forth in 45 C.F.R. § 164.304, "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system." Security Incident shall not include, (a) unsuccessful attempts to penetrate computer networks or servers maintained by Business Associate, or (b) immaterial incidents that occur on a routine basis, such as general "pinging" or "denial of service" attacks.
- k. Security Rule** shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and C.
- l. Unsecured PHI** shall have the meaning given to such term under the HITECH Act and any guidance issued pursuant to such Act including, but not limited to, 42 U.S.C. Section 17932(h)(1) and 45 C.F.R. § 164.402.

2. Duties & Responsibilities of Business Associate

- a. Permitted and Prohibited Uses.** Business Associate shall use Protected Information only for the purpose of performing Business Associate's obligations under the Agreement, as otherwise permitted or required under the Agreement, and for:

 - a. the proper management and administration of Business Associate, (ii) to carry out the legal responsibilities of Business Associate, or (iii) data aggregation purposes for the Health Care Operations of Covered Entity. [45 C.F.R. §§ 164.502(a)(3), 164.504(e)(2)(ii)(A) and 164.504(e)(4)(i)]. Further, Business Associate shall not use Protected Information in any manner that would constitute a violation of the Privacy Rule, the HITECH Act, or other applicable law if so used by Covered Entity.
- b. Permitted and Prohibited Disclosures.** Business Associate shall not disclose Protected Information except for the purpose of performing Business Associate's obligations under the Agreement, as permitted or required under the Agreement, and as required by law. Business Associate shall not disclose Protected Information in any manner that would constitute a violation of the Privacy Rule, the HITECH Act, or other applicable law if so disclosed by Covered Entity. However, Business Associate may disclose Protected Information (i) for the proper management and administration of Business Associate; (ii) to carry out the legal responsibilities of Business Associate; or (iii) for data aggregation purposes for the Health Care Operations of Covered Entity. If Business Associate discloses Protected Information to a third party, Business Associate must obtain, prior to making any such disclosure, (i) reasonable written assurances from such third party that such Protected Information will be held confidential as provided pursuant to this BAA and only disclosed as required by law or for the purposes for which it was disclosed to such third party, and (ii) a written agreement from such third party to immediately notify Business Associate of any Privacy Breaches of confidentiality of the Protected

Information within twenty-four (24) hours of discovery, to the extent it has obtained knowledge of such Privacy Breach. [42 U.S.C. §17932; 45 C.F.R. §§ 164.504(e)(2)(i)-(ii)(A) and 164.504(e)(4)(ii)].

- c. **Additional Prohibited Uses and Disclosures.** Business Associate shall not use or disclose Protected Information for fundraising or marketing purposes. [42 U.S.C. §17936(a) and 45 C.F.R. § 164.501]. Business Associate shall not disclose Protected Information to a health plan for payment or health care operations purposes if the individual has requested this special restriction, and has paid out of pocket in full for the health care item or service to which the Protected Information solely relates. [42 U.S.C. §17935(a); 45 C.F.R. §164.502(a)(5)(ii)]. Business Associate shall not directly or indirectly receive remuneration in exchange for Protected Information, except with the prior written consent of Covered Entity and as permitted by the HITECH Act. [42 U.S.C. §17935(d)(2)]. This prohibition shall not affect payment by Covered Entity to Business Associate for services provided pursuant to the Agreement.
- d. **Appropriate Safeguards.** Business Associate shall implement appropriate administrative, technological, and physical safeguards as are necessary to prevent the use or disclosure of Protected Information other than as permitted by this BAA that reasonably and appropriately protect the confidentiality, integrity, and availability of the Protected Information, and comply, where applicable, with the HIPAA Security Rule with respect to Electronic PHI. Business Associate, including any of its agents and subcontractors, shall not create, receive, maintain, transmit, or store Protected Information outside the United States.
- e. **Reporting of Improper Access, Use, or Disclosure.** Business Associate shall notify Covered Entity's Student Health Services (as detailed below) within twenty-four (24) hours of any suspected or actual Privacy Breach of Protected Information; any use or disclosure of Protected Information not permitted by this Agreement; any security incident (*i.e.*, any attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in any information system) related to Protected Information, and any actual or suspected use or disclosure of data in violation of any applicable federal or state laws by Business Associate or its agents or subcontractors.

- a. Business Associate shall report to contact below in writing any suspected or actual access, use, or disclosure of Protected Information not permitted by the Agreement, including this BAA, and any other applicable state or federal law, including, but not limited to 42 U.S.C. Section 17921; 45 C.F.R. §164.504(e)(2) (ii) (C); 45 C.F.R. §164.308(b); California Health & Safety Code Section 1280.15, California Confidentiality of Medical Information Act (California Civil Code Section 56.10) to the following contacts:

San Jose City College
Coordinator of Student Health Services
2100 Moorpark Ave. San Jose, CA 95128
408-288-3724

Evergreen Valley College
Director of Student Health & Wellness Services
3095 Yerba Buena Road. San Jose, CA 95135
408-274-7900 x6528

- b. Notification shall include, to the extent possible, the following: (1) a brief description of what happened, including the date of the suspected or actual Privacy Breach and/or Security Incident, and the date of the discovery of the Privacy Breach, if known and applicable; (2) the location of the breached information; (3) the unauthorized person who used the Protected Information or to whom the disclosure was made; (4) whether the Protected Information was actually acquired or viewed; (5) a description of the types of Protected Information that were involved in the Privacy Breach and/or Security Incident; (6) safeguards

in place prior to the Privacy Breach and/or Security Incident; (7) actions taken in response to the Privacy Breach and/or Security Incident; (8) any steps individuals should take to protect themselves from potential harm resulting from the Privacy Breach and/or Security Incident; (9) a brief description of what the business associate is doing to investigate the Privacy Breach and/or Security Incident, to mitigate harm to individuals, and to protect against further Privacy Breaches and/or Security Incidents; and (10) contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, and website or postal address. [45 C.F.R. §§164.410(c) and 164.404(c)]. Business Associate shall take any action pertaining to such actual or suspected Privacy Breach and/or Security Incident required by applicable federal and state laws and regulations, including 45 C.F.R. §164.410 with respect to reporting Privacy Breaches of Unsecured PHI. [42 U.S.C. §17921; 45 C.F.R. §§164.504(e)(2)(ii)(C), Section 164.308(b)]

- f. Business Associate's Agents and Subcontractors.** Business Associate shall ensure that any agents or subcontractors to whom it provides Protected Information agree in writing to the same restrictions and conditions that apply to Business Associate with respect to such Protected Information and implement the safeguards required by paragraph (II)(d) above with respect to Electronic PHI provided by Covered Entity or created or received on Covered Entity's behalf. [45 C.F.R. §§ 164.502(e)(1)(ii), 164.504(e)(2)(ii)(D) and 164.308(b)]. If Business Associate knows of a pattern of activity or practice of an agent or subcontractor that constitutes a material breach or violation of an agent or subcontractor's obligations under their contract or addendum or other arrangement with the agent or subcontractor, the Business Associate must take reasonable steps to cure the breach or end the violation. If these steps are unsuccessful, Business Associate shall sanction or terminate the contract or arrangement with agent or subcontractor, if feasible. [45 C.F.R. §164.504(e)(1)(iii)]. Business Associate shall provide written notification to Covered Entity of any pattern of activity or practice of a subcontractor or agent that Business Associate believes constitutes a material breach or violation of the agent or subcontractor's obligations under the contract or addendum or other arrangement with the agent or subcontractor within twenty four (24) hours of discovery and shall meet with Covered Entity to discuss and attempt to resolve the problem as one of the reasonable steps to cure the breach or end the violation.
- g. Access to Protected Information.** Business Associate shall make Protected Information maintained by Business Associate or its agents or subcontractors in Designated Record Sets available to Covered Entity for inspection and copying within ten (10) days of a request by Covered Entity to enable Covered Entity to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. §164.524. If Business Associate maintains an Electronic Health Record, Business Associate shall provide such information in electronic format to enable Covered Entity to fulfill its obligations under the HITECH Act, including, but not limited to, 42 U.S.C. Section 17935(e)(1). If any individual requests access to Protected Information Covered Entity in writing within five (5) days of the request.
- h. Electronic PHI.** If Business Associate receives, creates, transmits, or maintains ePHI on behalf of Covered Entity, Business Associate will, in addition, do the following:

 - a. Develop, implement, maintain, and use appropriate administrative, physical, and technical safeguards in compliance with Section 1173(d) of the Social Security Act, Title 42, Section 1320(s) or the United States Code and Title 45, Part 162 and 164 of C.F.R. to preserve the integrity and confidentiality of all ePHI received from or on behalf of Covered Entity.
 - b. Document and keep these security measures current and available for inspection by Covered Entity.

- c. Ensure that any agent, including a subcontractor, to whom the Business Associate provides ePHI received from or on behalf of Covered Entity, agrees to implement reasonable and appropriate safeguards to protect it.
 - d. Report to the Covered Entity, as provided in Section 2(d), any actual or suspected Privacy breach and/or Security Incident of which it becomes aware.
- i. **Amendment of Protected Information.** Within ten (10) days of receipt of a request from Covered Entity for an amendment of Protected Information or a record about an individual contained in a Designated Record Set, Business Associate or its agents or subcontractors shall make such Protected Information available to Covered Entity for amendment and incorporate any such amendment to enable Covered Entity to fulfill its obligations under the Privacy Rule. If any individual requests an amendment of Protected Information directly from Business Associate or its agents or subcontractors, Business Associate must notify Covered Entity in writing within five (5) days of the request. Any approval or denial of amendment of Protected Information maintained by Business Associate or its agents or subcontractors shall be the responsibility of Covered Entity.
- j. **Accounting Rights.** Business Associate agrees to document such disclosures of Protected Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an individual for an accounting of disclosures of PHI in accordance with the Privacy Rule and the HITECH Act. [42 U.S.C. § 17935(c) and 45 C.F.R. § 164.528]. Business Associate agrees to implement a process that allows for an accounting of disclosures to be collected and maintained by Business Associate and its agents or subcontractors for at least six (6) years prior to the request. Accounting of disclosures from an Electronic Health Record for treatment, payment or health care operations purposes are required to be collected and maintained for three (3) years prior to the request, and only to the extent Business Associate maintains an Electronic Health Record and is subject to this requirement.
 - a. At a minimum, the information collected and maintained shall include: (i) the date of disclosure; (ii) the name of the entity or person who received Protected Information and, if known, the address of the entity or person; (iii) a brief description of Protected Information disclosed and (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's authorization, or a copy of the written request for disclosure. [45 C.F.R. §164.528(b)]. In the event that the request for an accounting is delivered directly to Business Associate or its agents or subcontractors, Business Associate shall forward it to Covered Entity in writing within five (5) days of the request. It shall be Covered Entity's responsibility to prepare and deliver any such accounting requested. Business Associate shall not disclose any Protected Information except as set forth in the Agreement and this BAA.
- k. **Governmental Access to Records.** Business Associate shall make its internal practices, books, and records relating to the use and disclosure of Protected Information available to Covered Entity and to the Secretary of the U.S. Department of Health and Human Services (the "Secretary") for purposes of determining Business Associate's compliance with the Privacy Rule. [45 C.F.R. §164.504(e)(2)(ii)(I)]. Business Associate shall concurrently provide to Covered Entity a copy of any internal practices, books, and records relating the use and disclosure of Protected Information that Business Associate provides to the Secretary.
- l. **Minimum Necessary.** Business Associate and its agents or subcontractors shall request, use, and disclose only the minimum amount of Protected Information reasonably necessary to accomplish the purpose of the request, use, or disclosure in accordance with 42 U.S.C. Section 17935(b).
- m. **Protected Information Ownership.** Business Associate acknowledges that Business Associate has no ownership rights with respect to the Protected Information governed by this BAA, and all rights, interests, and title remain vested in the Covered Entity at all times.

- n. **Warranties and Disclosures.** Business Associate assumes risk for any and all use of Protected Information. Covered Entity assumes no liability or responsibility for any errors or omissions in, or reliance upon, the Protected Information, including, but not limited to information electronic systems. Covered Entity makes no representations or warranties of any kind, express or implied, including but not limited to: accuracy, completeness, or availability of content, non-infringement, merchantability, or fitness for a particular use or purpose. Covered Entity does not warrant that Protected Information is free of viruses or other harmful components or that service will be uninterrupted or error-free, or that defects will be corrected.
- o. **Audits, Inspection, and Enforcement.** Within ten (10) days of a written request by Covered Entity, Business Associate and its agents or subcontractors shall allow Covered Entity to conduct a reasonable inspection of the facilities, systems, books, records, agreements, policies, and procedures relating to the use or disclosure of Protected Information pursuant to this BAA for the purpose of determining whether Business Associate has complied with this BAA; provided, however, that (i) Business Associate and Covered Entity shall mutually agree in advance upon the scope, timing, and location of such an inspection; (ii) Covered Entity shall protect the confidentiality of all confidential and proprietary information of Business Associate to which Covered Entity has access during the course of such inspection; and (iii) Covered Entity shall execute a nondisclosure agreement, upon terms mutually agreed upon by the parties, if requested by Business Associate.
- a. The fact that Covered Entity inspects, or fails to inspect, or has the right to inspect, Business Associate's facilities, systems, books, records, agreements, policies, and procedures does not relieve Business Associate of its responsibility to comply with the BAA, nor does Covered Entity's (i) failure to detect any unsatisfactory practices; or (ii) detection, but failure to notify Business Associate or require Business Associate's remediation of any unsatisfactory practices; constitute acceptance of such practice or a waiver of Covered Entity's enforcement rights under the Agreement or BAA. Business Associate shall notify Covered Entity within five (5) days of learning that Business Associate has become the subject of an audit, compliance review, or complaint investigation by the Office for Civil Rights of the U.S. Department of Health and Human Services.
- p. **Termination**
- a. **Material Breach.** A Breach by Business Associate of any provision of this BAA shall constitute a material breach of the Agreement and shall provide grounds for immediate termination of the Agreement, notwithstanding any provision in the Agreement to the contrary. [45 C.F.R. §164.504(e)(2)(iii)].
- b. **Judicial or Administrative Proceedings.** Covered Entity may terminate the Agreement, effective immediately, if (i) Business Associate is named as a defendant in a criminal proceeding for a violation of HIPAA, the HITECH Act, the HIPAA Regulations or other security or privacy laws; or (ii) a finding or stipulation that the Business Associate has violated any standard or requirement of HIPAA, the HITECH Act, the HIPAA Regulations or other security or privacy laws is made in any administrative or civil proceeding.
- c. **Effect of Termination.** Upon termination of the Agreement for any reason, Business Associate shall, at the option of Covered Entity, immediately return or destroy all Protected Information that Business Associate or its agents or subcontractors still maintain in any form, and shall retain no copies of such Protected Information. If return or destruction is not feasible, Business Associate shall continue to extend the protections of Section II of the BAA to such information, and limit further use of such Protected Information to those purposes that make the return or destruction of such Protected Information infeasible. [45 C.F.R. § 164.504(e)(ii)(2)(I)]. If Covered Entity elects destruction of the

Protected Information, Business Associate shall certify in writing to Covered Entity that such Protected Information has been destroyed.

3. General Provisions

- a. **Indemnification.** In addition to the indemnification language in the Agreement, Business Associate agrees (i) to be responsible for, and defend, indemnify, and hold harmless the Covered Entity for any breach of Business Associate's privacy or security obligations under the Agreement, including any fines, penalties, and assessments that may be made against Covered Entity or the Business Associate for any Privacy Breaches or late reporting; and (ii) to pay and bear responsibility for the cost of and notice for any credit monitoring services.
- b. **Disclaimer.** Covered Entity makes no warranty or representation that compliance by Business Associate with this BAA, HIPAA, the HITECH Act, or the HIPAA Regulations will be adequate or satisfactory for Business Associate's own purposes. Business Associate is solely responsible for all decisions made by Business Associate regarding the use and safeguarding of PHI.
- c. **Amendment to Comply with Law.** The parties acknowledge that state and federal laws relating to data security and privacy are evolving and that amendment of the Agreement or BAA 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 Privacy Rule, the Security Rule and other applicable California laws relating to the security or confidentiality of PHI. Upon the request of any Party, the other Party agrees to promptly enter into negotiations concerning the terms of an amendment to the BAA embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule and other applicable California laws relating to the security or confidentiality of PHI. Covered Entity may terminate the Agreement between the Parties or the provisions of this BAA upon thirty (30) days written notice in the event (i) Business Associate does not promptly enter into negotiations to amend the Agreement when requested by Covered Entity pursuant to this section or (ii) Business Associate does not enter into an amendment to the Agreement providing assurances regarding the safeguarding of Protected Information that Covered Entity, in its sole discretion, deems sufficient to satisfy the standards and requirements of applicable laws.
- d. **Assistance in Litigation of Administrative Proceedings.** Business Associate shall notify Covered Entity within forty-eight (48) hours of any litigation or administrative proceedings commenced against Business Associate or its agents or subcontractors. Business Associate shall make itself, and any subcontractors, employees, or agents assisting Business Associate in the performance of its obligations under the Agreement, including this BAA, available to Covered Entity, at no cost to Covered Entity, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against Covered Entity, officers or employees based upon a claimed violation of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule, or other laws relating to security and privacy, except where Business Associate or its subcontractor, employee, or agent is named as an adverse party.
- e. **No Third-Party Beneficiaries.** Nothing express or implied in the Agreement, including this BAA, is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Business Associate, and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.
- f. **Effect on Agreement.** Except as specifically required to implement the purposes of the BAA, or to the extent inconsistent with this BAA, all other terms of the Agreement shall remain in force and effect.

- g. Interpretation.** The BAA shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, the Privacy Rule, and the Security Rule. The parties agree that any ambiguity in this BAA shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act, the Privacy Rule, and the Security Rule and other applicable California laws relating to the security or confidentiality of PHI.
- h. Governing Law, Venue.** This Business Associate Agreement has been executed and delivered in, and shall be construed and enforced in accordance with, the laws of the State of California. Proper venue for legal action regarding this Agreement shall be in the County of Santa Clara.
- i. Survivorship.** The respective rights and responsibilities of Business Associate related to the handling of Protected Information survive termination of this Agreement.

IN WITNESS HEREOF, the District and Consultant have executed this Agreement as of the dates set forth below.

FOR DISTRICT:	FOR BUSINESS ASSOCIATE:
Signature:	Signature:
Name:	Name:
Title:	Title:
Date:	Date:

*APPROVED Re: Form & Legality
By:
Date:

*MUST BE SIGNED BY THE DISTRICT IF
MODIFICATIONS MADE TO THIS AGREEMENT.