State of California
Interagency Data Exchange Agreement
And
Memorandum of Understanding

1. PARTIES

This Interagency Data Exchange Agreement (IDEA or Agreement) and Memorandum of Understanding is made between the Signatory Entities within the State of California and shall take effect immediately on the date of execution, as defined herein.

2. PURPOSE AND INTENT

This Agreement is intended to facilitate data exchange, in any form, between the Signatory Entities in compliance with all applicable federal, state and local laws, regulations, and policies. This Agreement is intended to be the sole agreement for data exchange among Signatory Entities and eliminates the need for Signatory Entities to enter into "point-to-point" agreements, except where a different agreement is required by federal or state law.

This Agreement sets forth a common set of terms, conditions, and obligations in support of secure interoperable data exchange between and among Signatory Entities. The Signatory Entities have agreed to receive and/or provide data from every data source system as necessary and have established information technology applications and infrastructure with which to share data to improve services to the residents of California. The Signatory Entities have agreed to facilitate the process of data exchange efficiently, within a reasonable timeframe.

The Signatory Entities recognize that many individuals living in California may qualify for and participate in more than one State program or service. Leveraging advances in technology and exchanging data will bridge information silos between Signatory Entities and provide the following benefits:

- Assure the privacy and security of data
- Improve consumer experiences and outcomes
- Increase reliability of data
- Reduce duplication of consumer data
- Improve integration of consumer services
- Promote a consumer-centric approach to service delivery
- Improve accessibility and management of information
- Improve program effectiveness, performance, and accountability.

3. SPECIAL COMPLIANCE PROVISIONS

3.1 Addendum A is incorporated herein by reference and sets forth terms and conditions for a Memorandum of Understanding required by the Health Insurance Portability and

Accountability Act of 1996 (HIPAA). It is understood and agreed that Addendum A of this Agreement shall be inapplicable to Signatory Entities that do not meet the definition of a covered entity or business associate, as those terms are defined in 45 C.F.R. § 160.103, or the definition of hybrid entity, as that term is defined in 45 C.F.R. § 164.103, and therefore does not impose HIPAA requirements or standards on non-covered entities or non-covered components of Signatory Entities unless they are business associates of covered entity Signatory Entities.

3.2 Addendum B is incorporated herein by reference and sets forth terms and conditions for access, use, and disclosure of student educational records and Data consistent with the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 C.F.R. Part 99). It is understood and agreed that Addendum B of this Agreement shall be inapplicable to Signatory Entities unless the Data being exchanged is covered by FERPA, therefore Addendum B does not impose FERPA requirements or standards on Signatory Entities unless the Data being exchanged is covered by FERPA.

4. DEFINITIONS

“Agency” means the term as defined in Government Code section 12855 and also includes Veteran Affairs and the Department of Food and Agriculture.

“Agency Chief Data Officer” means an Agency’s Chief Data Officer or the equivalent and is the person designated in a Signatory Entity to be responsible for facilitating review and decision on disputed Business Use Case Proposals.

“Agency Information Officer” means an Agency’s Chief Information Officer or the equivalent in a Signatory Entity that is not an Agency. The Agency Information Officer or the equivalent is the person designated in a Signatory Entity to be responsible for facilitating review and decision on disputed Business Use Case Proposals when the Signatory Entity does not have an Agency Chief Data Officer or the equivalent.

“Agreement” or “IDEA” means the Interagency Data Exchange Agreement and, unless otherwise specified, includes all approved or Undisputed Business Use Case Proposals, Addendum A, and Addendum B, all of which are incorporated herein by reference as if fully set forth in the Agreement.

“Authentication” is the process by which users accessing a system demonstrate that they are in fact a person or entity that is associated with an identity previously registered in the system. Authentication does not apply solely to users; it can also be applied at the system or service level (for example, by User Group or division) and can be used to identify one system or service to another. It includes verifying the identity of a user, process, or device, as a prerequisite to allowing access to resources in an information system.

“Authorization” or “Authorize” means the act of granting a user, program, process or device access to Data after proper identification and Authentication are obtained.

“Authorized User” means an individual who has been approved and designated by a Signatory Entity to access a Signatory Entity’s Data in connection with an undisputed or approved Business Use Case.

A “Business Use Case” is a description of the functions and responsibilities of a Signatory Entity or division and/or unit of a Signatory Entity, the Data requested, and the purpose and intended use of the Data.

A “Business Use Case Proposal” is a document containing the Business Use Case submitted for review and approval by a Data Recipient and/or Data Provider. Business Use Case Proposals that are objected to by a Data Provider are disputed and must be reviewed and approved prior to access, transmission, or receipt of any Data by a Signatory Entity.

“Certification” is written affirmation by a Data Recipient and/or Data Provider that its Data Protections meet the requirements of any applicable federal and state laws, regulations, and policies, including the State Administrative Manual, Chapter 5300.

The “Chief Data Officer” is the California State Chief Data Officer.

“Data” when capitalized herein means information collected or maintained by Signatory Entities that is exempt from disclosure under the provisions of the California Public Records Act (Government Code sections 6250 et seq.) or which has restrictions on disclosure in accordance with other applicable federal or state laws and is accessed or transmitted from one Signatory Entity to another Signatory Entity. Data includes but is not limited to a representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automated means. Data also includes metadata and data kept in any form, including paper, optical, or other media. It excludes de-identified data and public documents and data, as defined by the Public Records Act (Government Code section 6250 et seq.).

“Data Protection” means technologies deployed or data protection capabilities including, but not limited to: 1) specific access controls; 2) field by field redaction; 3) upstream and downstream filtering; 4) encryption; and 5) filtering logic to restrict quantity of data provided.

“Data Provider” means a Signatory Entity or unit or program within a Signatory Entity that provides Data from Data Source Systems or alternative-storage means to a Data Recipient.

“Data Recipient” means a Signatory Entity or unit or program within a Signatory Entity and its specific Authorized User Groups, which has been approved to access or receive Data from a Data Provider.

“Data Source Systems” or “Source Systems” are terms used interchangeably in this Agreement and mean individual electronic information storage systems for Data from

Data Providers.

“Dispute Resolution Process” means the process by which the Signatory Entities agree to resolve disputed Business Use Case Proposals.

“Permitted Uses” means the access to and use of Data provided pursuant to this Agreement is restricted to Authorized Users.

“Provisioning” refers to Data Recipients providing access privileges to Authorized Users. Provisioning is separate and distinct from the vetting process used to authorize a user to access Data.

“Required by Law” means a duty contained in law that compels a Signatory Entity to make use or disclosure of Data. Required by law includes, but is not limited to, federal and state court orders, statutes, or regulations.

“Signatory Entity” or “Signatory Entities” means every state office, officer, department, board, commission, entity, and Agency in California state government, including but not limited to entities defined under Article IV, Article V, Article VI, and Article IX of the California Constitution and Education Code sections 70900 et seq. and 89000 et seq., that has signed this Agreement.

“Undersecretary” means the Undersecretary of an Agency.

“Undisputed Business Use Case Proposal” means a Business Use Case Proposal that has not been objected to by a Data Provider.

“User Group” means a unit or program within a Data Recipient authorized to access information from a Data Provider’s Data Source Systems.

5. GENERAL PROVISIONS

5.1 Signatory Entities agree to collaborate on Business Use Cases and to work together to create Business Use Case Proposals as efficiently as possible. All Undisputed Business Use Case Proposals, including exchanges that are Required by Law, shall be provided to the Chief Data Officer by the Data Recipient.

5.2 A Data Recipient and a Data Provider shall collectively develop a Business Use Case Proposal. A Business Use Case Proposal may include, but is not limited to: (i) a brief description of each User Group's business function within its Signatory Entity, including key roles and responsibilities of staff; (ii) individual scenarios describing how staff would make use of the Data within their current business processes (such as how Authorized Users currently access these Data, if applicable, and the manner in which the Data are currently used); (iii) the purpose for which the Data would be used; (iv) a description of the added value and benefit of accessing the requested Data; and (v) any necessary additional security or restrictions on access and use of Data. Each Business Use Case

Proposal also includes an associated list of relevant data sources, data categories, and/or documents supporting business use case scenarios. As part of the Business Use Case Proposal, the Data Recipient shall briefly explain how and why the proposal is undisputed. An undisputed Business Use Case is automatically deemed approved. A Disputed Business Use Case shall go through the Dispute Resolution Process.

5.2 If a Data Provider objects to a Business Use Case Proposal and the dispute cannot be resolved, the Data Provider shall provide a written explanation for the objection(s) to the Agency Chief Data Officer or equivalent if applicable, or else the Agency Information Officer(s) or the equivalent. The explanation shall be considered during the Dispute Resolution Process. In the event the Signatory Entities are still unable to resolve the dispute, the Dispute Resolution Process under Section 6 of this Agreement shall apply.

5.3 Signatory Entities shall provide, access, and/or use Data only for approved purposes and only to the extent necessary, consistent with all applicable federal, state, and local laws; rules and regulations; and consistent with an undisputed or approved Business Use Case Proposal(s). Data shall be maintained as confidential and shall only be used for authorized purposes directly related to the carrying out of Authorized Users' functions and responsibilities consistent with an undisputed or approved Business Use Case Proposal. Authorized Users receive rights to access a Signatory Entity's Data from their individual Signatory Entity, which is solely responsible for the Provisioning and de-Provisioning of its employees, agents, contractors, and business associates. In granting access, a Signatory Entity affirms such individuals are authorized to access a particular type and quantity of Data based upon their functions and responsibilities and consistent with their undisputed or approved business use cases.

5.4 The Data Provider's Undersecretary or the equivalent shall determine access to data elements contained within Data Source System(s) based upon applicable laws, rules, regulations, contracts, and policies. Further, each Data Recipient shall have sole discretion to add additional access restrictions based upon applicable laws, rules, regulations, contracts, and business policies.

5.5 Signatory Entities are responsible for protecting the confidentiality and information security of Data accessed, transmitted, or received pursuant to this Agreement and shall implement administrative, physical, and technical safeguards based upon applicable federal and state laws, regulations, policies, or other rules that reasonably and appropriately protect the confidentiality, integrity, and availability of the Data that it creates, receives, maintains, or transmits.

5.6 Signatory Entities shall take all reasonable steps to maintain the confidentiality and information security of shared Data, which shall be subject to verification by the Data Provider. Further, Signatory Entities are responsible for overseeing the actions of their employees, agents, contractors and subcontractors with respect to the provision of, use of, and access to the Data that is shared pursuant to this Agreement.

5.7 Signatory Entities shall ensure in a written agreement that any agent, contractor, or

subcontractor to whom it provides Data agrees to implement reasonable and appropriate safeguards to protect and maintain such Data consistent with federal and state laws, including but not limited to, the Information Practices Act (Civil Code section 1798 et seq.) and applicable requirements of the State Administrative Manual Chapter 5300, this Agreement, and the Business Use Case Proposal.

5.8 Signatory Entities agree that their employees will access, use, and disclose Data consistent with their authorization(s) to participate and further agree to take appropriate action, which may include discipline and restrictions on access, where such authorization has been violated and/or misused.

5.9 Signatory Entities agree that all sharing of Data shall be in accordance with all applicable federal and state laws, rules, and regulations.

5.10 Signatory Entities are responsible for the maintenance of their own Data Source System.

5.11 A Signatory Entity may use another Signatory Entity's Data by modifying it consistent with an approved or Undisputed Business Use Case Proposal, either alone or in collaboration with a Signatory Entity. A Signatory Entity that modifies Data from another Signatory Entity shall disclose to users of the Data, particularly if de-identified and released as public data, that the Data is not original but modified.

5.12 Signatory Entities shall immediately remove an Authorized User's access to Source Systems if the Authorized User no longer qualifies as an Authorized User due to improper access, use, and/or disclosure.

5.13 Signatory Entities shall immediately remove an Authorized User's access to Source Systems if such Authorized User's role and responsibilities change and the user is no longer performing the functions of Permitted Uses consistent with the Signatory Entity's Business Use Case Proposal, or the Authorized User is no longer employed by the Signatory Entity.

5.14 Should a Data Provider stop exchanging Data with a Data Recipient based upon statutory, regulatory, or contractual changes, or based on the Data Recipient's acts in connection with Source Systems or this Agreement, the Data Provider shall immediately notify in writing the Agency Chief Data Officer if applicable, or else the Agency Information Officer(s) or the equivalent of the reasons in support of such action or if proposed but not yet taken, a request to take such action.

5.15 This Agreement eliminates the need for Signatory Entities to enter into individual agreements for Data exchange with each other for Data and purpose(s) associated with Source Systems and undisputed or approved Business Use Case Proposals, except where a different agreement is required by federal or state law.

5.16 Signatory Entities shall provide a Certification to the Chief Data Officer that

represents and affirms in writing that they have adequate Data Protection.

5.17 Business Use Case Proposals must be created for every access or transmission of Data, including disclosures that are Required by Law, and shall be forwarded to the Chief Data Officer by the Agency Chief Data Officer, if applicable, or else the Agency Information Officers or the equivalent for tracking and auditing purposes. To promote compliance with the provisions of this Agreement, the Chief Data Officer may collaborate with the following officers of the Signatory Entities: Chief Information Officers or the equivalent, Undersecretaries or the equivalent, Agency Chief Data Officers or the equivalent, Agency Information Officers or the equivalent, Privacy Officers, and internal governance entities. To improve state business processes or services, the Chief Data Officer shall also ensure records are maintained to track and evaluate all Business Use Case Proposals.

5.18 Confidential Data is accessed or transmitted under this Agreement pursuant to Government Code section 6254.5, including subdivision (e). Signatory Entities agree that in the event a Data Recipient receives a request under the California Public Records Act (CPRA), a subpoena, a court order, a litigation-related request, or any other request for the Data that is the subject of this Agreement, the Data Recipient shall immediately notify the Data Provider and meet and confer on the appropriate response to the request. The Data Provider shall communicate what Data is exempt from the CPRA and the applicable exemption(s) to the Data Recipient.

5.19 Signatory Entities may de-identify the Data that is the subject of this Agreement and use de-identified Data for any lawful purpose. Signatory Entities are responsible for ensuring the adequacy of the de-identification method before use to ensure that the de-identified Data cannot be linked to an individual that is the subject of the Data. De-identification methods include but are not limited to statistical suppression, complementary suppression, or masking algorithms. Prior to implementing the intended use of the de-identified Data, a Data Recipient shall provide to the Data Provider for review, the proposed de-identified Data to be used. If the Data Provider disagrees with the de-identification determination, the Data Provider shall notify the Data Recipient of its assessment and objections within five working days of receiving the de-identified Data. The Dispute Resolution Process in Section 6 shall be used if the Data Provider and Data Recipient cannot agree within 10 working days following the notification of objections to the de-identified Data.

5.20 Nothing in this Agreement or in the approved or Undisputed Business Use Case Proposals shall waive or diminish any privilege or protection as a result of disclosing confidential Data pursuant to this Agreement, regardless of whether the Data Provider has asserted, or is or may be entitled, to assert, such protection or privilege.

5.21 Signatory Entities are responsible for their own costs unless the frequency of requests to an individual Signatory Entity are unduly burdensome causing a serious impact to the Signatory Entity’s budget. If the Data Provider and Data Recipient cannot agree on costs, they shall use the Dispute Resolution Process in Section 6. The Data

Provider and Data Recipient shall address the access or transmission of Data consistent with this Agreement but address the transfer of funds in a separate Interagency Agreement.

6. DISPUTE RESOLUTION PROCESS

6.1 Disputed Business Use Case Proposals shall be resolved at the lowest level possible based on the escalation process identified below:

1) Between two or more Signatory Entities where all Data Providers are within the same Agency or different Agencies under the Authority of the Governor.
   a) The disputed Business Use Case Proposal shall be submitted to the Agency Chief Data Officer if applicable, or else the Agency Information Officer(s) to assess the risks and benefits of the proposal, in consultation with Agency General Counsel(s) and to mediate between the Data Provider and Data Recipient.
   b) If mediation cannot resolve the dispute, the Chief Data Officer shall collect written comments and recommendations on the disputed Business Use Case Proposal(s) from the Agency Chief Data Officer or Agency Information Officer(s) as applicable and submit the comments and recommendations to the Undersecretary or, if applicable, Undersecretaries, for decision. The Chief Data Officer shall mediate the dispute and may seek and gather additional information and consult with the California State Chief Information Officer, Agency General Counsel(s), Agency Information Officer(s) or other Agency designated Executive, and/or the Data Provider or Data Recipient.
   c) If the Undersecretary or, if applicable, Undersecretaries, cannot resolve the dispute, then the Chief Data Officer shall elevate the disputed Business Use Case Proposal to the Governor's Office for final decision and submit a written recommendation.

2) Between two or more Signatory Entities where the Data Provider is a Signatory Entity that is not under the authority of the Governor. The Chief Data Officer shall mediate the dispute and may seek and gather additional information and consult with the California State Chief Information Officer, General Counsels, Agency Information Officers or the equivalent, and/or the Data Provider or Data Recipient regarding a disputed Business Use Case Proposal. If mediation cannot resolve the dispute, then the Business Use Case Proposal will be deemed not approved and the dispute ended.

7. SPECIAL TERMS FOR DATA PROVIDERS

In addition to the terms and conditions set forth above for all Signatory Entities, each Data Provider additionally agrees to the following specific set of terms and conditions:

7.1 The Data Providers represent and affirm that they shall authorize access to Data by Authorized Users in accordance with all applicable federal, state, and local laws; rules, regulations, and policies; and that such Data may be shared pursuant to this Agreement consistent with the original purposes of its collection.

7.2 Data Providers agree to transmit their Data and, to the extent consistent with their governing statutes, regulations, existing contracts, rules and policies, to make such Data accessible in whole or in part for use by approved Data Recipients and their Authorized Users for purposes described in undisputed or approved Business Use Case Proposals.

7.3 When Data Providers use specialized security or privacy requirements unique to the Data beyond the requirements of this Agreement, which may be required by state or federal law, such as the Social Security Administration Act, Data Providers shall communicate these additional security measures to Data Recipients. Any additional security or privacy requirements shall be set forth within the Business Use Case Proposal. Data Recipients shall implement the additional security or privacy requirements consistent with the Business Use Case Proposal.

7.4 Data Providers may terminate access to a source system and/or transmission of Data to any Data Recipient if the Data Provider determines that the Data Recipient has violated a material term of this Agreement. A Data Provider terminating access to a source system and/or transmission of Data to a Data Recipient shall immediately notify in writing the Data Recipient and Chief Data Officer.

7.5 During development of a Business Use Case Proposal, a Data Provider may exclude certain Data and/or records based upon applicable laws, rules, contracts, policies, and/or regulations from a Business Use Case Proposal. However, Data Providers may not exclude Data on a disputed but approved Business Use Case Proposal.

7.6 Data Providers shall provide data definitions if Data will be sourced from them.

8. SPECIAL TERMS FOR DATA RECIPIENTS

In addition to the terms and conditions above set forth for all Signatory Entities, each Data Recipient additionally agrees to the following specific set of terms and conditions:

8.1 Data Recipients shall restrict access to Data and Source Systems to Authorized Users and only for authorized purposes, as described in undisputed or approved Business Use Case Proposals.

8.2 All Data shall be held confidential to the extent Required by Law, and shall only be used for authorized purposes directly related to carrying out the Authorized Users' functions and responsibilities consistent with the undisputed or approved Business Use Case Proposals.

8.3 Data Recipients shall ensure that Authorized Users are trained prior to accessing Data, including an explanation of the guidelines for access and use of Data, and privacy and information security requirements. Data Recipients shall also ensure Authorized Users receive updated training on a periodic basis.

8.4 Data Recipients shall use any necessary administrative, technical and physical safeguards to protect the confidentiality, integrity, and availability of Data.

8.5 Data Recipients shall immediately report in writing to a Data Provider any access, use, or disclosure of Data not permitted or required by this Agreement, or an undisputed or approved Business Use Case Proposal(s), or as Required by Law. The Data Recipient will provide the Data Provider with any information necessary for the Data Provider to make any legally required notification.

8.6 Data Recipients shall immediately report in writing to Data Providers any information security incident involving loss, theft, damage, misuse of information assets, or improper dissemination of Data of which it becomes aware. Data Recipients shall also immediately notify in writing to Data Providers of any access, use, or disclosure of Data inconsistent with this Agreement or the undisputed or approved Business Use Case Proposal(s) of which it becomes aware.

8.7 Data Recipients shall not further disclose Data unless Required by Law or as authorized in the undisputed or approved Business Use Case Proposal.

8.8 Upon termination of the business use case, the Data Recipient shall return or destroy the Data provided consistent with the undisputed or approved Business Use Case Proposal unless an alternative is provided in the undisputed or approved Business Use Case Proposal. If the Data cannot be returned or destroyed, the Data Recipient shall continue to safeguard the information and limit further uses or disclosures. If circumstances change and, as a result, the Data cannot be returned or destroyed consistent with the approved Business Use Case Proposal, the Data Recipient must inform the Data Provider and Chief Data Officer within 10 days of an alternative method with a description of Data Protections. In the event Data Provider continues to provide any Data to Data Recipient after the expiration or termination of this Agreement, Data Recipient shall continue to protect all such Data received and limit use or disclosure of the Data in accordance with the provisions of this Agreement, and all applicable state and federal laws.

8.9 Due to the differences in collection practices that are specific to individual program needs, requests for Data about a particular consumer may not always yield Data with the identification demographics provided. It is possible that demographics and identifying information collected by one Signatory Entity differs from demographics and identifying information collected by another. Unless prohibited by law, the Signatory Entities shall work together as reasonably necessary on identifying consumers based on information and demographics when it is likely a consumer receives services from more than one Signatory Entity.

8.10 Each Data Recipient shall ensure that Authorized Users understand that improper use or disclosure is in violation of such Signatory Entity's policies and will result in appropriate action, including potential disciplinary action, and may also subject such employee to civil or criminal penalties.

9. CONSUMER NOTIFICATION

9.1 In the event any individual, including a California resident, whose unencrypted personal information was acquired or reasonably believed to have been acquired by an unauthorized person, the Signatory Entities shall follow all federal and state laws related to consumer notification, including but limited to, Civil Code section 1798.29.

9.2 In the event of a large security breach that requires notice to the California Attorney General, the Signatory Entity that is required by federal or state law shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the California Attorney General. If federal or state law does not specify which Signatory Entity must provide notice to the Attorney General, then the Signatory Entity that experienced the breach shall provide the notice.

10. NO WARRANTIES

10.1 The exchanged Data is provided by the Data Provider to the Data Recipient(s) without any warranties, express or implied, including without limitation any warranty of fitness for a particular use.

11. CONTROLLING LAWS, RULES, AND REGULATIONS

11.1 Signatory Entities are responsible for tracking changes in applicable law. Notwithstanding any prior approvals regarding the sharing of Data, if a change is required regarding authorized use(s) to comply with statutory and/or regulatory changes, Signatory Entities shall notify the Agency Information Officer or the equivalent to implement such change in compliance with all applicable laws, rules, and regulations. All Business Use Case Proposals are required to be amended in the event of a change in law, when necessary to comply with applicable law. Signatory Entities shall work together to amend a Business Use Case Proposal when necessary.

12. IMPROPER USE AND DISCLOSURE

12.1 Any individual who has engaged in improper use or disclosure of Data will be subject to their Signatory Entity's disciplinary process. Any individual who has engaged in improper use or disclosure of Data may be subject to civil and/or criminal penalties.

12.2 Signatory Entities shall immediately remove an Authorized User's access to Data or a Source System if the Authorized User has engaged in improper use and/or disclosure of Data and/or Source Systems. Signatory Entities shall have policies and procedures addressing the protocol for investigating and removing access when an Authorized User is suspected of engaging in improper use and/or disclosure. Signatory Entities shall follow their internal policies and procedures when an Authorized User is suspected of engaging in improper use and/or disclosure.

13. DISCLAIMERS

13.1 Nothing in this Agreement shall be deemed to impose responsibility or liability on a Signatory Entity related to the accuracy, content, or completeness of any Data provided pursuant to this Agreement.

13.2 The Signatory Entities acknowledge that other Signatory Entities may be added or terminated at any time; therefore, Signatory Entities may not rely upon the continued availability of a particular Signatory Entity's Data.

13.3 NO THIRD PARTY BENEFICIARIES. Nothing express or implied in the terms and conditions of this Agreement or its incorporated Business Use Case Proposals is intended to confer, nor shall anything herein confer, upon any person other than the Signatory Entities and their respective successors or assignees, any rights, remedies, obligations, or liabilities whatsoever.

14. SECURITY

14.1 Multiple technologies shall be deployed with Data Protection capabilities by Signatory Entities that meet, at a minimum, standards in Chapter 5300 of the State Administrative Manual, including: 1) role based access controls; 2) field by field redaction where applicable; 3) upstream and downstream firewall filtering; 4) encryption of Data in motion; 5) encryption of Data at rest on end points; 6) filtering logic to restrict quantity of Data provided; and 7) auditing. Signatory Entities certify they have in place a system that provides policy-based Authentication and Authorization of users. Access is obtained only by individuals whose credentials are verified upon log-in and have been approved by their Signatory Entity. Each source system shall filter Data based upon Authorized Users assigned role and Agency. Activities will be recorded in security audit logs. All use will be subject to compliance with a Signatory Entity's policies and procedures for data access, use, and disclosure.

15. SEVERABILITY

15.1 If any paragraph, term, condition or provision of this Agreement is found by a court of competent jurisdiction to be invalid or unenforceable, or if any paragraph, term, condition, or provision, is found to violate or contravene the substantive laws of the State of California, then that paragraph, term, condition or provision found to be invalid or unenforceable shall be deemed severed from this Agreement and all other paragraphs, terms, conditions and provisions shall remain in full force and effect.

16. ADDITIONAL SIGNATORY ENTITIES

16.1 The Signatory Entities acknowledge that additional Signatory Entities (Data Providers and/or Data Recipients) may be added to this Agreement. All current Signatory Entities agree that, prior to admission of a new Signatory Entity, the new Signatory Entity must agree to be bound by the terms of this Agreement. An additional Signatory Entity,

if not a current signatory, shall stipulate in writing to all the terms of this Agreement. The Signatory Entities agree that upon such stipulation by a duly authorized representative of the additional Signatory Entity, such additional Signatory Entity shall be deemed to be a signatory to this Agreement and will be bound by all the terms of this Agreement. All such stipulations shall be incorporated by reference as if fully set forth herein.

17. EFFECTIVE DATE

17.1 This Agreement shall be effective as to a Signatory Entity on the date signed by a duly authorized representative of the Signatory Entity, and shall remain in full force and effect, unless terminated or otherwise modified as provided herein.

18. MODIFICATION / TERMINATION

18.1 This Agreement may only be modified or terminated in writing by mutual consent of the Agencies' Secretaries or highest-ranking executive in the Signatory Entities. Approved or Undisputed Business Use Case Proposals may be modified by Signatory Entities without the need to modify this Agreement. Modified, approved, or Undisputed Business Use Case Proposals shall automatically be incorporated by reference into this Agreement upon execution of the involved Signatory Entities.

19. ELECTRONIC COPY

19.1 The Signatory Entities agree that a copy of the original signatures, including an electronic copy, may be used for any and all purpose for which the original signature may be used.

20. ENTIRE AGREEMENT

20.1 This Agreement, along with any addenda, amendments hereto, and approved Business Use Case Proposals, encompass the entire and integrated agreement of the parties, and supersedes any and all previously written or oral understandings and agreements between the parties, respecting the subject matter hereof.

21. COUNTERPARTS

21.1 This Agreement and any amendments to it may be executed in counterparts, and all of these counterparts together shall be deemed to constitute one and the same Agreement.

22. SIGNATURES

The undersigned are party representatives duly authorized to execute this Agreement, including all its terms, conditions, and obligations. By signing, the authorized party representatives acknowledge they understand the Agreement and hereby accept and agree to be bound by all the provisions and terms and conditions set forth in this Interagency Data Exchange Agreement.

Original signed by:

Ana Matosantos
Cabinet Secretary, Governor’s Office

Lourdes Castro Ramírez
Secretary, Business, Consumer Services and Housing Agency

Josh Fryday
Chief Service Officer, California Volunteers

Kathleen Allison
Secretary, Department of Corrections & Rehabilitation

Keely Bosler
Director, Department of Finance

Karen Ross
Secretary, Department of Food & Agriculture

Vito Imbasciani, MD
Secretary, Department of Veteran's Affairs

Jared Blumenfeld
Secretary, Environmental Protection Agency

Yolanda Richardson
Secretary, Government Operations Agency

Chris Dombrowski
Acting Director, Governor’s Office of Business and Economic Development

Mark Ghilarducci
Director, Governor’s Office of Emergency Services

Kate Gordon
Director, Governor’s Office of Planning and Research

Christina Snider
Director, Governor’s Office of the Tribal Advisor

Mark Ghaly, MD
Secretary, Health & Human Services Agency

Julie Su
Secretary, Labor & Workforce Development Agency

Major General David S. Baldwin
Adjutant General, Military Department

Wade Crowfoot
Secretary, Natural Resources Agency

Brooks Allen
Executive Director, State Board of Education

David S. Kim
Secretary, State Transportation Agency

ADDENDUM A

MEMORANDUM OF UNDERSTANDING FOR
HIPAA COVERED ENTITIES AND BUSINESS ASSOCIATES

1. This Addendum only applies to Signatory Entities that meet the definition of covered entity or business associate as defined in 45 C.F.R. § 160.103 or that meet the definition of hybrid entity as defined in 45 C.F.R. § 164.103.

2. The federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires a Memorandum of Understanding between governmental entities with respect to the receipt, access, use and disclosure of protected health information as defined in 45 C.F.R. § 160.103. The covered entity Signatory Entities and their business associate Signatory Entities intend this Agreement to act as the Memorandum of Understanding pursuant to 45 C.F.R. § 164.504(e)(3)(i)(A).

3. This Agreement further sets forth the obligations of Signatory Entities that access, use, and disclose protected health information. It is understood and agreed that the Memorandum of Understanding portion of this Agreement is not intended to apply to Signatory Entities that do not meet the definition of a covered entity or business associate, as those terms are defined in 45 C.F.R. § 160.103, or the definition of hybrid entity, as that term is defined in 45 C.F.R. § 164.103, and therefore it does not impose HIPAA requirements or standards on non-covered entity or non-covered components of Signatory Entities unless they are business associates of covered entity Signatory Entities.

4. "Covered entity", "business associate" and "protected health information" shall have the same meaning as defined in 45 C.F.R. § 160.103. “Hybrid entity” shall have the same meaning as defined in 45 C.F.R. § 164.103. "Covered component" shall have the same meaning as "health care component" as defined in 45 C.F.R. § 164.103. "Security incident" shall have the same meaning as defined in 45 C.F.R. § 164.304. "Breach" shall have the same meaning as defined in 45 C.F.R. § 164.402.

5. The covered entity and business associate Signatory Entities agree to the following:

5.1. Signatory Entities are responsible for protecting the confidentiality of protected health information and shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of protected health information that it creates, receives, maintains, or transmits consistent with federal laws and standards and the State Administrative Manual Chapter 5300.

6. Data Providers and/or Data Recipients shall ensure in a written agreement that any agent, contractor, or subcontractor to whom it provides protected health information, agrees to implement reasonable and appropriate safeguards to protect Data consistent with federal and state laws, including but not limited to, the Information Practices Act and HIPAA. This Agreement shall satisfy this requirement between Signatory Entities.

7. Data Providers may terminate access to a Source System and/or transmission of Data to any Data Recipient if the Data Provider determines that the Data Recipient has violated a material term of this Agreement. A Data Provider terminating access to a Source System and/or transmission of Data to a Data Recipient shall immediately notify the Data Recipient in writing.

8. Data Recipients shall use any necessary administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of Data transmitted or accessed from Source Systems. Data Recipient business associates shall comply with Subpart C of 45 C.F.R. Part 164 with respect to protected health information to prevent use and disclosure not permitted or required by this Agreement, approved or Undisputed Business Use Case Proposal(s), or as Required by Law.

9. A Data Recipient business associate shall immediately report in writing to a Data Provider covered entity any security incident or breach of which it becomes aware. Data Recipient business associates shall also immediately notify Data Provider covered entities in writing of any use or disclosure of Data inconsistent with this Agreement or the approved or Undisputed Business Use Case Proposal(s) of which it becomes aware.

10. A Data Recipient shall not further disclose Data unless Required by Law or consistent with applicable approved or Undisputed Business Use Case Proposals.

11. Data Recipient business associates shall make available protected health information to patients when requested in accordance with 45 C.F.R. § 164.524. Data Recipient business associates shall make available protected health information for amendment and incorporate amendment in accordance with 45 C.F.R. § 164.526. Data Recipient business associates shall also make available the information required to provide an accounting of disclosures in accordance with 45 C.F.R. § 164.528. If applicable, Data Providers shall notify Data Recipient of any patient preferences regarding methods of how to communicate with the patient.

12. With respect to protected health information, Data Recipient business associates agree to use and disclose Data only as permitted or required by the approved or Undisputed Business Use Case Proposal(s) or as Required by Law.

13. When an approved or Undisputed Business Use Case Proposal or other obligation requires a Data Recipient business associate to carry out a covered entity Data Provider's obligation under Subpart E of 45 C.F.R. Part 164, the Data Recipient business associate shall comply with the requirements of Subpart E that apply to the Data Provider covered entity in performance of its obligations to the Data Provider covered entity.

14. Data Recipient business associates shall make their practices, personnel, books, records, and policies regarding the use and disclosure of protected health information available to the Secretary of the federal Health and Human Services when requested to determine the compliance of the Data Provider covered entity.

15. Data Recipient business associates shall ensure in a written agreement that contractors, consultants, and subcontractors that create, receive, store, or transmit protected health information on behalf of the Data Recipient agree to the same restrictions, requirements, conditions that apply to the Data Recipient with respect to protected health information.

16. Upon termination of the Business Use Case as approved in the Business Use Case Proposal the Data Recipient shall return or destroy the Data provided consistent with the approved or Undisputed Business Use Case Proposal. If the Data cannot be returned or destroyed, the Data Recipient shall continue to safeguard the information and cease further uses or disclosures. If circumstances change and, as a result, the Data cannot be returned or destroyed consistent with the approved or Undisputed Business Use Case Proposal(s), the Data Recipient must inform the Data Provider within 10 days of an alternative method with description of Data Protections.

ADDENDUM B

FERPA for Educational Records

1. APPLICATION AND INTERPRETATION:

1.1. The provisions of this Addendum B shall apply to all disclosures or redisclosures of education records containing personally identifiable information.

1.2.The Family Educational Rights and Privacy Act (FERPA) definitions set forth in 34 CFR 99.3 shall be used to interpret the meaning of this Agreement, including the terms “education records,” “authorized representative,” “disclosure,” “educational agency or institution,” “education program,” and “personally identifiable information.”

1.3. Each Business Use Case Proposal (BUCP) that involves the disclosure or redisclosure of education records must:

a. specify the personally identifiable information from education records to be disclosed;
b. specify the purpose for which the personally identifiable information from education records is to be disclosed, including a citation to the applicable subsection within 34 CFR 99.31 that exempts the disclosure from requiring written consent;
c. A description of the activity with sufficient specificity to make clear that the work falls within the cited exception of § 99.31, including a description of how the personally identifiable information from education records will be used; and
d. include any additional covenants, statements, agreements or other pre-requisites for disclosure, including, without limitation, any applicable prerequisites set forth in 99 CFR 99.35. This includes, but is not limited to:
    i. Designating the Data Recipient as an authorized representative of the Data Provider, as required by FERPA;
    ii. Including a requirement that the Data Recipient destroy personally identifiable information from education records when the information is no longer needed for the purpose specified;
    iii. Specifying the time period in which the information must be destroyed;
    iv. Set forth the policies and procedures, consistent with FERPA and other Federal and State confidentiality and privacy provisions, that have been established to protect personally identifiable information from education records from further disclosure (except back to the disclosing entity) and unauthorized use, including limiting use of personally identifiable information from education records to only authorized representatives with legitimate interests in the audit or evaluation of a Federal- or State-supported education program or for compliance or enforcement of Federal legal requirements related to these programs; and

v. Be revised to include the most current data security and other terms and conditions that are required by the Data Provider to assure by the Data Recipient complies with applicable law;

e. Include a covenant by the Data Recipient to store and maintain the data so it may be destroyed at any time and to do so when required by the Data Provider.

1.4. Each BUCP that involves the disclosure or redisclosure of education records must be approved and signed by the education agency who is a Signatory Entity to this agreement who is the original source of such education records.

2. AUDITS AND EVALUATIONS

2.1. Data Recipient may receive educational records containing personally identifiable information from Data Provider if the Data is used for purposes of auditing or evaluating federal or state-supported educational programs or for the enforcement of or compliance with federal legal requirements that relate to those programs as permissible pursuant to FERPA. The BUCP must specify how these audit and evaluation requirements are being met and how the Data Recipient will assure ongoing compliance.

2.2. In particular, the Data Recipient must specify in the Business Use Case Proposal the scope of the audit or evaluation, the schedule for the audit or evaluation, the number and type of reports or other deliverables, the primary contacts for each Party, the education program to be audited or evaluated, the identity of all individuals that will have access to the Data and the methodology that is proposed to conduct the audit or evaluation, including any proposed data linkages. The description of the methodology must contain enough detail so that the Data Provider can determine if the requested Data elements are being used in a valid and sound manner, based on data qualities, attributes, collection methods and definitions.

2.3. For purposes of sharing student-level educational records with Data Recipient for auditing or evaluating federal or state-supported educational programs or for the enforcement of or compliance with federal legal requirements that relate to those programs. Data Provider hereby appoints Data Recipient as its authorized representative pursuant to 20 U.S. Code section 1232g(b)(1)(C)(i)(III). Data Recipient hereby accepts its appointment as Data Provider's authorized representative for purposes of receiving student-level educational records and agrees to abide by FERPA and all applicable state and federal laws in connection with its use and disclosure of such records.

2.4. Data Recipient acknowledges that its appointment as an authorized representative may create a fiduciary relationship prohibiting certain conflicts of interest that should be addressed in the Business Use Case Proposal.

2.5. The appointment of Data Recipient as Data Provider's authorized representative may not be assigned or otherwise transferred to another entity.

3. RESEARCH AGREEMENTS

3.1. Data Recipient may receive educational records containing personally identifiable information from Data Provider if the Data is used by qualified researchers at state agencies and the University of California, California State University or the Chancellor of the California Community Colleges, provided that such entities pay the fees required, if any, under Education Code section 49079.7.

3.2. Data Recipient may receive educational records containing personally identifiable information from Data Provider if the Data is used for:

a. studies
b. conducted for or on behalf of educational agencies or institutions
c. in order to:
    i. Develop, validate, or administer predictive tests;
    ii. Administer student aid programs; or
    iii. Improve instruction;

3.3. The BUCP must specify how these studies requirements are being fulfilled and how the Data Recipient will assure ongoing compliance.

3.4. In particular, the Data Recipient must specify in the BUCP, as the case may be, the scope of the study, the schedule for the study, the number and type of study reports or other deliverables, the primary contacts for each Signatory Entity, the educational agency or institution on whose behalf the study will be conducted, the predictive test to be developed, validated or administered, the student aid program to be administered or the instruction to be improved, the identity of all individuals that will have access to the Data and the methodology that is proposed to conduct the study. The description must contain enough detail so that the Data Provider can determine if the requested data elements are being used in a valid and sound manner, based on data qualities, attributes, collection methods and definitions.

3.5. Data Recipient agrees to provide the Data Provider with an advance electronic copy of all study report(s) at least sixty (60) calendar days prior to release for the following purposes:

a. To confirm the description and the use of the methodology set forth in the BUCP or as otherwise agreed by the Data Provider and Data Recipient(s);
b. To review for factual errors with respect to descriptions of data provided by the Data Provider;
c. To ensure the confidentiality of any schools and Local Education Agencies (LEAs) included in the study;
d. To ensure proper de-identification and confidentiality of student data with small cell sizes (i.e., groups of ten (10) or fewer students); and
e. To review for errors in assumptions, logic, or conclusions, misleading or confusing statements, and other substantive concerns.

3.6. The Data Provider shall provide written comments, if any, to Data Recipient within forty-five (45) calendar days of receipt of the advance copy. The Data Recipient may then take an additional fifteen (15) calendar days to address the Data Provider's comments.

3.7. Data Recipient agrees to include in the study report(s) a footnote fully disclosing Data Provider's concerns, if not satisfactorily resolved by the review process.

3.8. Data Recipient acknowledges that conducting research for or on behalf of an educational agency or institution may create a fiduciary relationship prohibiting certain conflicts of interest that should be addressed in the BUCP.

4. GENERAL PROVISIONS APPLICABLE TO ALL DISCLOSURES OF EDUCATION RECORDS

4.1. The Data Recipient must use the education records data only as described in the BUCP, including adherence to any schedule, methodology or other representation made. Data Recipient must notify the Data Provider of any delays to the schedule as they occur. The Data Recipient must destroy all educational records containing personally identifiable information within the time frame as stated in the Business Use Case Proposal or when the records are no longer needed to complete the purpose of the disclosure. Destruction of the referenced data must be witnessed by two people who can later attest that a complete, confidential destruction of the data occurred, including any derivative data which contains personally identifiable information. Data Recipient disclaims any and all rights or interests in or to any education records disclosed to it under this Agreement.

4.2. The Data Recipient shall establish policies and procedures, consistent with FERPA and other federal and state law, which protects the student-level educational records from unauthorized and further disclosure, including provision that these records are accessed, used, and disclosed only by authorized representatives with legitimate interest in the audit or evaluation of the education program. The Data Recipient shall comply with any Data Security Protocol attached to the Business Use Case Proposal.

4.3. The Data Recipient shall ensure that student-level educational records are protected from unauthorized and further disclosure and shall ensure that the records are accessed, used, and disclosed only by authorized representatives with legitimate interest in the audit or evaluation of the education program.