EDMUND G. BROWN JR.
GOVERNOR

State of California
HEALTH AND HUMAN SERVICES AGENCY

DIANA S. DOOLEY
SECRETARY

Aging

Child Support Services

Community Services and Development

Developmental Services

Emergency Medical Services Authority

Health Care Services

Managed Health Care

Office of Patient Advocate

Office of System Integration

Public Health

Rehabilitation

Social Services

State Hospitals

Statewide Health Planning and Development

CHHS Memorandum of Understanding and Intra-Agency Data Exchange Agreement

This Memorandum of Understanding and Intra-Agency Data Exchange Agreement (Agreement) is intended to facilitate data integration and exchange between departments within the California Health and Human Services Agency (CHHS) 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 CHHS Departments and eliminates the need for CHHS Departments to enter into "point-to-point" agreements except where a different agreement is required by the federal government or federal law.

This Agreement sets forth a common set of terms and conditions in support of secure interoperable data exchange between and among CHHS Departments. The undersigned CHHS Departments have agreed to receive and/or provide data from every CHHS data source system as necessary, and have established information technology applications and infrastructure with which to share data to improve services to the citizens of California.

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 by 45 C.F.R. § 160.103. The undersigned covered entity CHHS Departments and their business associate CHHS Departments hereby sign this Agreement to act as the Memorandum of Understanding as allowed by 45 C.F.R. § 164.504(e)(3)(i)(A).

This Agreement further sets forth the obligations of CHHS Departments 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 CHHS Departments that do not meet the definition of a covered entity or business associate, as those terms are defined within 45 C.F.R. § 160.103, or the definition of hybrid entity, as that term is defined within 45 C.F.R. § 164.103, and therefore does not impose HIPAA requirements or standards on non-covered entity or non-covered components of CHHS Departments unless they are business associates of covered entity CHHS Departments.

The undersigned CHHS Departments recognize that many Californians qualify for and participate in multiple State programs. Leveraging advances in technology will break down information silos within CHHS Departments and provide the following benefits:

- Assure the privacy and security of data
- Improve consumer 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

I. DEFINITIONS/DEFINED TERMS

a. Authentication. Authentication is the process by which a user accessing a system demonstrates that (s)he is 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, department) 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.

b. Authorization or Authorize. The act of granting a user, program, process or device access to data after proper identification and authentication are obtained.

c. Authorized User. The term Authorized User is used to identify individuals approved and designated to access a CHHS data source system. Authorized Users receive rights to access a CHHS data source system from their individual CHHS Department which is solely responsible for the provisioning and de-provisioning of its employees, agents, contractors, and business associates. In granting access, such CHHS Department affirms such individuals are authorized to access the particular type and quantity of information based upon their functions and responsibilities consistent with their undisputed or approved business use cases.

d. Business Use Case. A business use case includes a description of the functions and responsibilities of a CHHS Department or division and/or unit of a CHHS Department, the information requested, and the purpose and intended use of the information. A business use case may include, but is not limited to: (i) a brief description of each user group's business function within its department, 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 workers 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;

and (iv) a description of the added value and benefit of accessing the requested data. Each use case also includes an associated list of relevant data sources, data categories, and/or documents supporting use case scenarios.

e. Business Use Case Proposal. Proposal of a business use case submitted for review and approval by a Data Recipient and/or Data Provider prior to transmission of data. Business Use Case Proposals that are objected to by a Data Provider are disputed and must be reviewed and approved prior to transmission or receipt of any data by a CHHS Department unless the transfer or receipt of data is required by law or in the event the data are essential for a CHHS Department to comply with the law. Review and approval shall be completed by the Risk Management Subcommittee. The Risk Management Subcommittee shall attempt to mediate the dispute between the Data Provider and Data Recipient. If it appears to the Risk Management Subcommittee that no compromise can be reached between the disputing CHHS Departments, then the CHHS Agency Information Officer and the CHHS General Counsel will elevate the disputed Business Use Case Proposal to the Undersecretary for final decision. Business Use Case Proposals must be created for every transmission of data, including disclosures that are required by law, for tracking and auditing purposes. (See Section III, Terms and Conditions)

f. Certification. Certification is written affirmation by a Data Recipient and/or Data Provider that its data protections meet the requirements in federal and state law, regulations, and policy, including the State Administration Manual, Chapter 5300.

g. CHHS Departments. Referred to collectively as the departments and offices within and including the California Health and Human Services Agency as defined by California Government Code § 12803.

h. CHHS Risk Management Subcommittee. The Risk Management Subcommittee serves as the main decision making body responsible for assessing the strategic relevance, business value, and potential liability of Business Use Case Proposals. The Risk Management Subcommittee's composition shall be determined and modified as needed by the Undersecretary. The Risk Management Subcommittee receives disputed Business Use Case Proposals from the Governance Liaison. The Risk Management Subcommittee shall approve, modify, or deny a disputed Business Use Case Proposal and explain why. The Risk Management Subcommittee shall refer a disputed Business Use Case Proposal to the Governance Liaison for review by other Governance Subcommittees when appropriate. The Governance Liaison shall collect and submit comments and recommendation on disputed Business Use Case Proposals from other Governance Advisory Subcommittees and provide them to the Risk Management Subcommittee for consideration. The Risk Management Subcommittee may seek and gather additional information from either the Data Provider or Data Recipient regarding a submitted Business Use Case Proposal. The Risk Management Subcommittee shall attempt to mediate the dispute between the Data Provider and Data Recipient. If it appears to the Risk Management Subcommittee that no compromise can be reached between the

disputing CHHS Departments, then the CHHS Agency Information Officer and the CHHS General Counsel will elevate the disputed Business Use Case Proposal to the Undersecretary for final decision. The Risk Management Subcommittee shall provide recommendations to the Undersecretary for consideration.

i. Data. As used in this Agreement, data shall mean any and all personal information, as defined by the California Information Practices Act at section 1798.3 of the Civil Code, that are transmitted from one CHHS Department to another CHHS Department, including but 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. It excludes departmental personnel records, held as employment records. It may also exclude de-identified data and public documents and data, as defined by the Public Records Act (Cal. Government Code § 6250 et seq.).

j. Data Protection. Multiple 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.

k. Data Provider. A Data Provider is a CHHS Department or unit or program within a CHHS Department that provides data from specified data source systems to a Data Recipient.

l. Data Recipient. A Data Recipient is a CHHS Department or unit or program within a CHHS Department and its specific Authorized User groups, which have been approved to access or receive data from a Data Provider.

m. Data Source Systems or CHHS Source Systems. Data Source Systems are individual data source system(s) that are electronic information storage systems for data elements or information from Data Providers.

n. Governance Liaison. The Governance Liaison is the Deputy Agency Information Officer who is responsible to facilitate review and decision on disputed Business Use Case Proposals. Data Recipients and Data Providers shall submit disputed Business Use Case Proposals to the Governance Liaison for facilitation through the review and decision process. The Governance Liaison shall refer all disputed Business Use Case Proposals to the CHHS Risk Management Subcommittee for decision. The Governance Liaison may independently refer a disputed Business Use Case Proposal to CHHS Governance Advisory Subcommittees for review and recommendations when appropriate. The Governance Liaison shall collect and submit comments and recommendations on disputed Business Use Case Proposals from CHHS Governance Advisory Subcommittees to the CHHS Risk Management Subcommittee. The Governance Liaison shall track all Business Use Case Proposals and evaluate the tracking log for trends and use the tracking log to improve CHHS business processes.

o. Permitted Uses. Access to and use of data provided by way of this Agreement a is restricted to Authorized Users. 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 undisputed or approved Business Use Case Proposal(s).

p. Provisioning. 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.

q. Required by Law. As used in this Agreement, required by law means a mandate contained in law that compels a CHHS Department to make a use or disclosure of data. Required by law includes, but is not limited to, court orders, statutes, and/or regulations.

r. Undisputed Business Use Case Proposal. An undisputed Business Use Case Proposal is a Business Use Case Proposal that has not been objected to by a Data Provider. The Data Recipient shall briefly explain how and why the matter is undisputed as part of the Business Use Case Proposal. Undisputed Business Use Case Proposals do not need to go through the formal vetting approval process. A Business Use Case is automatically considered approved if undisputed.

s. User Group. A unit or program within a Data Recipient authorized to access information from Data Provider data source systems. Access is based upon the undisputed or approval of a Business Use Case Proposal. Access shall be consistent with the undisputed or approved Business Use Case Proposal(s).

t. "Covered entity", "business associate", "hybrid entity", and "protected health information" shall have the same meaning as defined in 45 C.F.R. § 160.l 03. "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.

II. DATA EXCHAGE AGREEMENT TERMS AND CONDITIONS

A. This section establishes the terms and conditions related to CHHS Department responsibilities regarding the provision of data by Data Providers, and the access to and use of data by Data Recipients, when shared through any CHHS applications or infrastructure, as specified.

The undersigned CHHS Departments agree to the following terms and conditions:

1. CHHS Departments agree to collaborate on Business Use Cases and work together to create Business Use Case Proposals. All undisputed Business Use

Case Proposals, including exchanges that are required by law, shall be provided to the Governance Liaison by the Data Recipient.

2. If a Data Provider objects to a business use case, the objecting Data Provider shall provide an explanation for the objection to a Business Use Case Proposal to the Governance Liaison. The explanation provided shall be considered during the vetting process.

3. Each CHHS Department shall provide, access, and/or use the data only for permitted purposes and only to the extent necessary, consistent with all applicable federal, state, and local laws; rules and regulations; and consistent with the CHHS Department 's undisputed or approved Business Use Case Proposal(s).

4. The CHHS Risk Management Subcommittee and/or the Undersecretary shall have discretion to determine access to data elements contained within CHHS 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, beyond any imposed by the Risk Management Subcommittee, and based upon applicable laws, rules, regulations, contracts, and business policies.

5. Each CHHS Department is responsible for protecting the confidentiality of data and shall implement administrative, physical, and technical safeguards based upon applicable laws, regulations, policies, or other rules that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic data that it creates, receives, maintains, or transmits.

6. CHHS Departments shall take all reasonable steps to maintain the security of shared data. Further, each CHHS Department is responsible for overseeing the actions of its employees with respect to the provision of, use of, and access to the data that is shared pursuant to this Agreement.

7. CHHS Departments shall also 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 CHHS data consistent with federal and state laws, including but not limited to, the Information Practices Act and applicable requirements of the State Administration Manual Chapter 5300.

8. Each CHHS Department agrees that its employees will conduct business consistent with their authorization(s) to participate and further agrees to take appropriate action, which may include discipline and restrictions on access, where such authorization has been violated and/or misused.

9. Each CHHS Department agrees that all sharing of data shall be in accordance with all applicable laws, rules, and regulations.

10. Each CHHS Department is responsible for the maintenance of its own data source system.

11. Each CHHS Department shall only modify its own data.

12. CHHS Departments shall immediately remove an Authorized User's access to CHHS source systems if the Authorized User no longer qualifies as an Authorized User due to improper access, use, and/or disclosure.

13. CHHS Departments shall immediately remove an Authorized User's access to CHHS 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 CHHS Department's Business Use Case Proposal, or the Authorized User is no longer employed by the CHHS Department.

14. Should a CHHS Department stop exchanging data with another CHHS Department based upon statutory, regulatory, or contractual changes, or based on such other CHHS Department' s acts in connection with CHHS source systems or this Agreement , the CHHS Department shall immediately notify the Governance Liaison and the Risk Management Subcommittee of the reasons in support of such action or if proposed but not yet taken, a request to take such action.

15. This Agreement eliminates the need for CHHS Department s to enter into "point-to-point" agreements with each other for the same data and purpose(s) associated with CHHS source systems and undisputed or approved Business Use Case Proposals, except where a different agreement is required by the federal government or federal law regarding use and sharing of data obtained by the federal government that is shared with CHHS Departments.

16. CHHS Departments that intend to be Data Providers and/or Data Recipients shall provide a Certification to the Governance Liaison and the Risk

Management Subcommittee that represents and affirms in writing they have adequate data protection consistent with federal and state laws and regulations.

B. In addition to the terms and conditions above set forth for all CHHS Departments, each Data Provider and Data Recipient additionally agrees to the following specific set of terms and conditions:

Data Providers

1. The undersigned 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 without consumer consent.

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.

3. When Data Providers use specialized security requirements unique to the data in excess of the baseline described herein, that may be required by federal agencies such as the Social Security Administration, Data Providers shall communicate these additional security measures to Data Recipients. Any additional security requirements shall be set forth within the Business Use Case Proposal as part of the proposal. Data Recipients shall implement the additional security requirements consistent with the Business Use Case Proposal.

4. Data Providers may terminate access to a CHHS 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 CHHS source system and/or transmission of data to a Data Recipient shall immediately notify the Governance Liaison and the Risk Management Subcommittee.

5. Data Providers may exclude certain data and/or records based upon applicable laws, rules, contracts, and/or regulations. However, Data Providers may not exclude data on a disputed but approved Business Use Case Proposal.

6. Data Providers are expected to maintain their own data, and provide data definitions if data will be sourced from them.

Data Recipients

1. No Use by Other than Authorized Users. Data Recipients shall restrict access to data and CHHS source systems to Authorized Users and only for authorized purposes, as described in undisputed or approved Business Use Case Proposals.

2. All information accessed from CHHS source systems shall be held confidential to the extent required by law, and shall only be used for authorized purposes directly related to the carrying out the Authorized Users' functions and responsibilities consistent with Data Recipient' s undisputed or approved Business Use Case Proposals.

3. Each Data Recipient shall ensure that Authorized Users are trained prior to accessing a CHHS source system, explanation of the guidelines for access and use of data, and security requirements and the proper handling and use of data. Each Data Recipient shall also ensure Authorized Users receive updated training on a periodic basis.

4. Each Data Recipient shall use any necessary administrative, technical and physical safeguards to protect the confidentiality, integrity, and availability of data accessed from CHHS source systems.

5. Each Data Recipient shall immediately report to a Data Provider and the Governance Liaison 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.

6. Each Data Recipient shall immediately report to a Data Provider and Governance Liaison 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 Data Providers of any use or disclosure of data inconsistent with this Agreement or the undisputed or approved Business Use Case Proposal(s) of which it becomes aware.

7. Each Data Recipient shall not further disclose data unless required by law or as authorized in the Data Recipient's undisputed or approved Business Use Case Proposals.

8. Data Recipients shall ensure in written contract that contractors, consultants, and subcontractors that create, receive, store, or transmit data on behalf of the Data Recipient agree to the same restrictions, requirements, conditions that apply to the Data Recipient with respect to data.

9. At 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 stated 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 disclosure to those

purposes that make return or destruction infeasible. If circumstances change and, as a result, the data cannot be returned or destroyed consistent with the approved Business Use Case Proposal(s), the Data Recipient must inform the Data Provider, Governance Liaison, and Risk Management Subcommittee within 10 days of an alternative method with a description of data protections.

10. Due to the differences in collection practices that are specific to individual departmental 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 Department differs from demographics and identifying information collected by another. Departments shall work together on identifying information and demographics when it is likely a consumer receives services from more than one Department.

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

III. MEMORANDUM OF UNDERSTANDING FOR HIPAA COVERED ENTITIES AND BUSINESS ASSOCIATES

This portion of the Agreement only applies to CHHS Departments that meet the definition of covered entity or business associate as defined at 45 C.F.R. § 160.103 or that meet the definition of hybrid entity as defined at 45 C.F.R. § 164.103.

The undersigned covered entity and business associate CHHS Departments agree to the following:

1. Each Department is responsible for protecting the confidentiality of data 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 Administration Manual Chapter 5300.

2. 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 the Health Insurance Portability and Accountability Act. This Agreement shall satisfy this requirement between CHHS Departments.

3. Data Providers may terminate access to a CHHS 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 CHHS source system and/or transmission of data to a Data Recipient shall immediately notify the Governance Liaison and the Risk Management

Subcommittee.

4. Each Data Recipient shall use any necessary administrative, technical and physical safeguards to protect the confidentiality, integrity, and availability of data accessed from CHHS source systems. Business associate Departments that are Data Recipients 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, undisputed or approved Business Use Case Proposal(s), or as required by law.

5. Each business associate that is a Data Recipient shall immediately report in writing to a Data Provider and the Governance Liaison any security incident and breach of which it becomes aware. Business associate Departments that are Data Recipients shall also immediately notify Data Providers of any use or disclosure of data inconsistent with this Agreement or the undisputed or approved Business Use Case Proposal(s) of which it becomes aware.

6. A Data Recipient shall not further disclose data unless required by law or consistent with the Data Recipient's undisputed or approved Business Use Case Proposals.

7. Business associate department s that are Data Recipients shall make available protected health information to patients when requested in accordance with 45 C.F.R. § 164.524. Business associate Departments that are Data Recipients shall make available protected health information for amendment and incorporate amendment in accordance with 45 C.F.R. § 164.526. Business associate Departments that are Data Recipients shall also make available the information required to provide an accounting of disclosures in accordance with 45 C.F.R. § 164.528.

8. With respect to protected health information, business associate Departments that are Data Recipients agree to use and disclose data only as permitted or required by the undisputed or approved Business Use Case Proposal(s) or as required by law.

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

10. A business associate that is a Data Recipient shall make its 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 covered entity Data Provider.

11. Business associate Departments that are Data Recipients shall ensure in written contract that contractors, consultants, and subcontractors that create, receive, store, or transmit protected health information on behalf of the business associate that is a Data Recipient agree to the same restrictions, requirements, conditions that apply to the business associate that is a Data Recipient with respect to protected health information.

12. At 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 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 disclosure to those purposes that make return or destruction infeasible. If circumstances change and, as a result, the data cannot be returned or destroyed consistent with the undisputed or approved Business Use Case Proposal(s), the Data Recipient must inform the Data Provider and Governance Liaison within 10 days of an alternative method with description of data protections.

IV. CONTROLLING LAWS, RULES, AND REGULATIONS

Change Required to Comply with Applicable Law. Notwithstanding any prior approvals regarding the sharing of information, if a change is required regarding authorized use(s) to comply with statutory and/or regulatory changes, CHHS Departments shall notify the Governance Liaison and the Risk Management Subcommittee to implement such change in compliance with all applicable laws, rules and regulations. All impacted CHHS Departments shall be notified by the Governance Liaison and the Risk Management Subcommittee in the event of a change required to comply with applicable law. Business Use Case Proposals are required to be updated in the event of a change in law, when necessary to comply with applicable law.

V. IMPROPER USE AND DISCLOSURE

1. Access to CHHS data source systems is restricted to Authorized Users.

2. All data accessed from a CHHS source system shall be held confidential to the extent required by law, and shall be used by Authorized Users solely for carrying out their functions and responsibilities as Authorized Users directly related to and consistent with Data Recipient's undisputed or approved Business Use Case Proposal(s) .

3. Improper use or disclosure is in violation of CHHS Policy and applicable laws, rules, and regulations.

4. Any individual who has engaged in improper use or disclosure of CHHS source system data will be subject to his or her Department's disciplinary process.

5. Any individual who has engaged in improper use or disclosure of CHHS source system data may be subject to civil and/or criminal penalties.

6. CHHS Departments shall immediately remove an Authorized User's access to a CHHS source system if the Authorized User has engaged in improper use and/or disclosure. CHHS Departments 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. CHHS Departments shall follow their internal policies and procedures when an Authorized User is suspected of engaging in improper use and/or disclosure.

7. Required Notice to Data Providers: Should data obtained from a CHHS source system be improperly released (for example, misplaced or stolen, or disclosed in an unauthorized manner) or where the Data Recipient discovers evidence of willful or intentional misuse of data, the Data Recipient shall inform the Governance Liaison, the Risk Management Subcommittee, and the Data Provider whose data has been improperly released or misused immediately upon discovery by the Data Recipient.

VI. DISCLAIMERS

Reliance on a Data Source System: Nothing in this Agreement shall be deemed to impose responsibility or liability on a CHHS Department related to the accuracy, content, or completeness of any data provided pursuant to this Agreement. The CHHS Departments acknowledge that other CHHS Departments may be added or terminated at any time; therefore, CHHS Departments may not rely upon the continued availability of a particular CHHS Department's data.

VII. SECURITY

Multiple technologies shall be deployed with data protection capabilities on CHHS source systems, 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. Each CHHS Department certifies it has 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 CHHS Department. Each source system filters 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 CHHS and CHHS Departmental policies and procedures for data access, use, and disclosure.

VIII. SEVERABILITY

The provisions of this Agreement are severable. If any provision of this Agreement is held invalid, by any court that invalidity shall not affect the other provisions of this Agreement and the invalid provision(s) shall be considered modified to conform to the existing law.

IX. ADDITIONAL CHHS DEPARTMENTS

The undersigned CHHS Departments acknowledge that additional CHHS Departments (Data Providers and/or Data Recipients) may be added to this Agreement. All current CHHS Departments agree that, prior to admission of a new CHHS Department, the new CHHS Department must agree to be bound by the terms of this Agreement. An additional CHHS Department, if not a current signatory, shall stipulate to all the terms of this Agreement. The CHHS Department s agree that upon such stipulation by a duly authorized representative of such additional CHHS Department, such additional CHHS Department shall be deemed to be a signatory to this Agreement and will be bound by all the terms of this Agreement.

X. EFFECTIVE DATE

This Agreement shall remain in full force and effect immediately from the date of execution by a duly authorized representative of a CHHS Department.

XI. MODIFICATION / TERMINATION

This Agreement may only be modified or terminated in writing by mutual consent of all signing CHHS Departments.

XII. ENTIRE AGREEMENT

All undisputed and approved Business Use Case Proposals are incorporated by reference herein. No verbal agreement shall, in any way, vary or alter any provision of this Agreement. Aside from undisputed or approved Business Use Case Proposals, this written Agreement:

- Contains all the terms and conditions agreed upon by the parties hereto.
- Constitutes the full and complete agreement between the CHHS Departments.

No other written agreement shall, in any way, vary or alter any provision of this Agreement unless modified in writing by mutual consent of all CHHS Departments or as required by statutory or regulatory changes.

XIII. SIGNATURES

The undersigned hereby accept and agree to be bound by all of the provisions and terms and conditions set forth in this Intra-Agency Data Exchange Agreement.

Original signed by
_____Date 5/12/16
Diana Dooley, Secretary, California Health and Human Services Agency

Original signed by
_____Date 5/12/16
Michael Wilkening, Undersecretary, California Health and Human Services Agency

Original signed by
_____Date 5/16/16
Scott Christman, Agency Information Office (Acting), California Health and Human Services Agency

Original signed by
_____Date 5/12/16
Lora Connolly, Director, Department of Aging

Original signed by Mark Beckley for Alisha Griffin
_____Date 5/12/16
Alisha Griffin, Director, Department of Child Support Services

Original signed by
_____Date 5/12/16
Linné Stout, Director, Department of Community Services and Development

Original signed by
_____Date 5/12/16
Nancy Bargmann, Director, Department of Developmental Services

Original signed by
_____Date 5/12/16
Jennifer Kent, Director, Department of Health Care Services

Original signed by
_____Date 5/12/16
Shelley Rouillard, Director, Department of Managed Health Care

Original signed by
_____Date 5/12/16
Dr. Karen Smith, Director, Department of Public Health

Original signed by

_____Date 5/12/16

Joe Xavier, Director, Department of Rehabilitation

Original signed by

_____Date 5/12/16

Will Lightbourne, Director, Department of Social Services

Original signed by

_____Date 5/12/16

Pam Ahlin, Director, Department of State Hospitals

Original signed by Daniel Smiley for Howard Backer

_____Date 5/12/16

Howard Backer, M.D., Director, Emergency Medical Services Authority

Original signed by

_____Date 5/12/16

Elaine Scordakis, Assistant Director, Office of Health Information Integrity

Original signed by

_____Date 5/16/16

Ken Baird, Chief, Office of Law Enforcement Support

Original signed by

_____Date 5/12/16

Elizabeth Abbot, Director, Office of the Patient Advocate

Original signed by Fran Mueller for Robert David

_____Date 5/12/16

Robert P. David, Director, Office of Statewide Health Planning and Development

Original signed by

_____Date 5/12/16

John Boule, Director, Office of Systems Integration