Center for Infectious Diseases
General Data Use and Disclosure Agreement

This Center for Infectious Diseases General (CIDG) Data Use and Disclosure Agreement (Agreement) is entered into between the California Department of Public Health (CDPH) and Local Health Jurisdiction San Bernardino County Department of Public Health (Recipient). CDPH and Recipient may be referred to in this Agreement individually as "Party" and collectively as "Parties." By entering into this Agreement, the Parties agree to protect the privacy and provide security protections for all CIDG Data (as defined herein) in compliance with all state and federal laws applicable to the CIDG Data. Permission to collect, receive, Use, and Disclose CIDG Data requires execution of this Agreement which describes the terms, conditions, and limitations of Recipient's collection, receipt, Use, and Disclosure of the CIDG Data.

I. Order of Precedence: With respect to information privacy and security requirements for all CIDG Data, the terms and conditions of this Agreement shall take precedence over any conflicting terms or conditions set forth in any other agreement between Recipient and CDPH.

II. Effect on Lower Tier Transactions: The terms of this Agreement shall apply to all applicable contracts, subcontracts, subawards, and the information privacy and security requirements Recipient is obligated to follow with respect to CIDG Data disclosed to Recipient pursuant to Recipient's agreement with CDPH. When applicable Recipient shall incorporate the relevant provisions of this Agreement into each subcontract or subaward to its agents, subcontractors, or independent consultants.

III. System Exhibits: The Parties agree to comply with the terms and conditions of the following selected Exhibits, which by this reference are made a part of this Agreement. The Parties understand and agree that changes to existing Exhibits or additions of new Exhibits can be added through mutual agreement in writing directed to the parties in XIII(g) below and do not require amendment of this Agreement:

☑ Exhibit A – California Connected (CalCONNECT) Terms
☑ Exhibit B – California Immunization Registry (CAIR) Terms
☑ Exhibit C – California Reportable Disease Information Exchange (CalREDIE) Terms
☑ Exhibit D – Integrated Infectious Disease Data Warehouse (I2D2) Terms
☑ Exhibit E – My Turn Vaccine Management System
☑ Exhibit F – CalREDIE Cross-Jurisdictional Data Sharing Authorization
☑ Exhibit G – CalCONNECT Cross-Jurisdictional Data Sharing Authorization

IV. Definitions: For purposes of the Agreement between Recipient and CDPH, the following definitions shall apply:

a. Breach: "Breach" means:

i. the unauthorized acquisition, access, Use, or Disclosure of CIDG Data in a manner which compromises the security, confidentiality, or integrity of the information; or

ii. the same as the definition of "breach of the security of the system" set forth in California Civil Code section 1798.29, subdivision (f). The "system" referenced in Civil Code section 1798.29 shall be interpreted for purposes of this Agreement to reference the specific system for which an LHJ signs onto as attached in Exhibits A-G.

b. Confidential Information: "Confidential Information" means information that:

   i. does not meet the definition of "public records" set forth in California Government Code section 7920.530, or

   ii. is exempt from Disclosure under any of the provisions of Government Code section 7920.000, et seq. or any other applicable state or federal laws; or

   iii. is contained in documents, files, folders, books, or records that are clearly labeled, marked, or designated in writing with the word "confidential" by CDPH.

c. CIDG Data: "CIDG Data" means any Personal Information or Confidential Information, as defined herein, which is accessed from, maintained in, transferred to, transferred from the systems listed in the Exhibits attached to this Agreement to which the Parties have agreed.

d. Disclosure: "Disclosure" means the release, transfer, provision, access, or divulging in any manner of information outside the entity holding the information.

e. Personal Information: "Personal Information" means information, in any medium (paper, electronic, oral) that:

   i. directly identifies or uniquely describes an individual; or

   ii. could be Used in combination with other information to indirectly identify or uniquely describe an individual, or link an individual to the other information; or

   iii. meets the definition of "personal information" set forth in Civil Code section 1798.3, subdivision (a); or

   iv. meets the definition of "personal information" set forth in Civil Code section 1798.29, subdivision (g)(1) or (g)(2); or

   v. meets the definition of "medical information" set forth in either Civil Code section 1798.29, subdivision (h)(2) or Civil Code section 56.05, subdivision (j); or

   vi. meets the definition of "health insurance information" set forth in Civil Code section 1798.29, subdivision (h)(3); or

   vii. is protected from Disclosure under applicable state or federal law.

f. Security Incident: "Security Incident" means:

   i. an attempted Breach;

   ii. the attempted or successful unauthorized access or Disclosure, modification, or destruction of CIDG Data, in violation of any state or federal law or in a manner not permitted under this Agreement;

   iii. the attempted or successful modification or destruction of, or interference with, Recipient's system operations in an information technology system, that negatively impacts the confidentiality, availability, or integrity of CIDG Data;

iv. any event that is reasonably believed to have compromised the confidentiality, integrity, or availability of an information asset, system, process, data storage, or transmission;

v. an event that constitutes a violation or imminent threat of violation of information security policies or procedures, including acceptable use policies; or

vi. The term "Security Incident" shall not include pings and other broadcast attacks on Recipient's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in any defeat or circumvention of Recipient's IT security infrastructure or in any unauthorized access to, or Use, or Disclosure of, CIDG Data.

g. Use: "Use" means the sharing, employment, application, utilization, examination, or analysis of information for any purposes including publication.

h. Workforce Member(s): "Workforce Member(s)" means an employee, contractor, agent, volunteer, trainee, or other person whose conduct, in the performance of work for Recipient, is under the direct control of Recipient, whether or not they are paid by Recipient. Pursuant to state policy, Workforce Member(s) must only be located in the continental United States.

i. [Reserved]

V. Disclosure Restrictions: Recipient and its Workforce Member(s) shall protect from unauthorized Disclosure all CIDG Data. Recipient shall not disclose, except as otherwise specifically permitted by this Agreement between Recipient and CDPH, any CIDG Data to anyone other than CDPH personnel or programs without prior written authorization from the CDPH Program Contract Manager, except if Disclosure is otherwise permitted or required by state or federal law. For purposes of this Agreement, "Disclosure" does not include a disclosure to a Party's authorized Workforce Member(s).

VI. Use Restrictions: Recipient and its Workforce Member(s) shall not Use any CIDG Data for any purpose other than performing Recipient's obligations under this Agreement or as permitted under the individual Exhibits executed between the Parties for each individual system, or as otherwise permitted or required by state or federal law. Any other Use is strictly prohibited. Any Use of CIDG Data shall be limited to the minimum necessary, to the extent practicable, in carrying out the Recipient's obligations under this Agreement or the Exhibits.

VII. Health Insurance Portability and Accountability Act of 1996 (HIPAA) Authority:

a. CDPH and the Center for Infectious Disease (CID) HIPAA Status: CDPH is a "hybrid entity" for purposes of applicability of the federal regulations entitled "Standards for Privacy of Individually Identifiable Health Information" ("Privacy Rule") (45 C.F.R. Parts 160, 162, and 164) promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (42 U.S.C. §§ 1320d - 1320d-8) (as amended by Subtitle D Privacy, of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111–5, 123 Stat. 265–66)). None of the systems to which this agreement or the attached Exhibits are connected are designated by CDPH as, and are not, one of the HIPAA-covered "health care components" of CDPH. (45 C.F.R. § 164.105 (a)(2)(i)(B).) The legal basis for this determination is as follows:

i. The systems are not a component of CDPH that would meet the definition of a covered entity or business associate if it were a separate legal entity. (45 C.F.R. §§ 160.105(a)(2)(iii)(D); 160.103 (definition of "coveredentity")); and

ii. The HIPAA Privacy Rule creates a special rule for a subset of public health activities whereby HIPAA cannot preempt state law if, "[t]he provision of state law, including state procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention."(45 C.F.R. § 160.203(c) [HITECH Act, § 13421, sub. (a)].) [NOTE: See State laws and regulations listed in the attached Exhibits];

b. Parties Are "Public Health Authorities:" CDPH and Recipient are each a "public health authority" as that term is defined in the Privacy Rule. (45 C.F.R. §§ 164.501; 164.512(b)(1)(i).)

c. Data Use and Disclosure Permitted by HIPAA: To the extent a Disclosure or Use of CIDG Data may also be considered a Disclosure or Use of "Protected Health Information" (PHI) of an individual, as that term is defined in Section 160.103 of Title 45, Code of Federal Regulations, the following Privacy Rule provisions apply to permit such Data Disclosure and/or Use by CDPH and Recipient, without the consent or authorization of the individual who is the subject of the PHI:

i. HIPAA cannot preempt state law if, "[t]he provision of state law, including state procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct ofpublic health surveillance, investigation, or intervention." (45 C.F.R. § 160.203(c) [HITECH Act, § 13421, sub. (a)].) [NOTE: See state laws and regulations listed in the attached Exhibits];

ii. A covered entity may disclose PHI to a "public health authority" carrying out public health activities authorized by law; (45 C.F.R. § 164.512(b).);

iii. A covered entity may Use or disclose protected health information to the extent that such Use or Disclosure is required by law and the Use or Disclosure complies with and is limited to the relevant requirements of such law." (Title 45 C.F.R. §§ 164.502 (a)(1)(vii), 164.512(a) (1).) and,

iv. Other, non-public health-specific provisions of HIPAA may also provide the legal basis for all or specific CIDG Data Uses and Disclosures.

d. No HIPAA Business Associate Agreement or Relationship Between CDPH and Recipient: This Agreement, the Exhibits, and the relationship they memorialize between CDPH and Recipient do not constitute a business associate agreement or business associate relationship pursuant to Title 45, CFR, Part 160.103 (definition of "business associate"). The basis for this determination is Section 160.203(c) of Title 45 of the Code of Federal Regulations (see, also, HITECH Act, § 13421, subdivision. (a).) [NOTE: See state laws and regulations listed in the Exhibits attached hereto]. Accordingly, this Agreement and the Exhibits are not intended to nor at any time shall result in or be interpreted or construed as to create a business associate relationship between CDPH and Recipient. By the execution of this Agreement and the Exhibits, CDPH and Recipient

expressly disclaim the existence of any business associate relationship.

VIII. Safeguards: Recipient shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the privacy, confidentiality, security, integrity, and availability of CIDG Data, including electronic or computerized CIDG Data. At each location where CIDG Data exists under Recipient's control, Recipient shall develop and maintain a written information privacy and security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of Recipient's operations and the nature and scope of its activities in performing this Agreement, and which incorporates the requirements of Section VII, Security, below. Recipient shall provide CDPH with Recipient's current and updated policies within five (5) business days of a request by CDPH for the policies.

IX. Security: Recipient shall take any and all steps reasonably necessary to ensure the continuous security of all computerized data systems containing CIDG Data. These steps shall include, at a minimum:

a. Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III- Security of Federal Automated Information Systems, and/or NIST 800-53 (version 4 or subsequent approved versions) which sets forth guidelines for automated information systems in Federal agencies; and

b. in case of a conflict between any of the security standards contained in any of the aforementioned sources of security standards, the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to the CIDG Data from Breaches and Security Incidents.

X. Security Officer: At each place where CIDG Data is located, Recipient shall designate a Security Officer to oversee its compliance with this Agreement and to communicate with CDPH on matters concerning this Agreement.

XI. Training: Recipient shall provide training on its obligations under this Agreement, at its own expense, to all of its Workforce Member(s) who assist in the performance of Recipient's obligations under Recipient's agreement with CDPH, or who otherwise Use or Disclose CIDG Data.

a. Recipient shall require each employee who receives training to certify, either in hard copy or electronic form, the date on which the training was completed.

b. Recipient shall retain each employee's certifications for CDPH inspection for a period of three (3) years following contract termination or completion.

c. Recipient shall provide CDPH with its employee's certifications within five (5) business days of a request by CDPH for the employee's certifications.

XII. Workforce Member Discipline: Recipient shall impose discipline that it deems appropriate (in its sole discretion) on such employees and other Recipient Workforce Member(s) under Recipient's direct control who intentionally or negligently violate any provisions of this Agreement.

XIII. Recipient Breach and Security Incident Responsibilities:

a. Notification to CDPH of Breach or Security Incident: Recipient shall notify CDPH **immediately by telephone call and email** upon the discovery of a Breach, and **within twenty-four (24) hours by email** of the discovery of any Security Incident, unless a law enforcement agency determines that the notification will impede a criminal investigation, in which case the notification required by this section shall be made to CDPH immediately after the law enforcement agency determines that such notification will not compromise the investigation. Notification shall be provided to the CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer, using the contact information listed in Section XIII(g), below. If the Breach or Security Incident is discovered after business hours or on a weekend or holiday and involves CIDG Data in electronic or computerized form, notification to CDPH shall be provided by calling the CDPH Information Security Office at the telephone numbers listed in Section XIII(g), below. For purposes of this Section, Breaches and Security Incidents shall be treated as discovered by Recipient as of the first day on which such Breach or Security Incident is known to Recipient, or, by exercising reasonable diligence would have been known to Recipient. Recipient shall be deemed to have knowledge of a Breach if such Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is an employee, Workforce Member or agent of Recipient.

   Recipient shall take:

   i. prompt action to immediately investigate such Breach or Security Incident;

   ii. prompt corrective action to mitigate any risks or damages involved with the Breach or Security Incident and to protect the operating environment; and

   iii. any action pertaining to a Breach required by applicable federal and state laws, including, specifically, Civil Code section 1798.29.

b. Investigation of Breach and Security Incidents: Recipient shall immediately investigate such Breach or Security Incident. As soon as the information is known and subject to the legitimate needs of law enforcement, Recipient shall inform the CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer of:

   i. what data elements were involved, and the extent of the data Disclosure involved in the Breach, including, specifically, the number of individuals whose Personal Information was Breached;

   ii. a description of the unauthorized persons known or reasonably believed to have improperly Used the CIDG Data and/or a description of the unauthorized persons known or reasonably believed to have improperly accessed or acquired the CIDG Data, or to whom it is known or reasonably believed to have had the CIDG Data improperly disclosed to them;

   iii. a description of where the CIDG Data is believed to have been improperly Used or Disclosed;

   iv. a description of the probable and proximate causes of the Breach or Security Incident; and

v. whether Civil Code section 1798.29 or any other federal or state laws requiring individual notifications of Breaches have been triggered.

c. Written Report: Recipient shall provide a written report of the investigation to the CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer as soon as practicable after the discovery of the Breach or Security Incident. The report shall include, but not be limited to, the information specified above, as well as a complete, detailed corrective action plan, including information on measures that were taken to halt and/or contain the Breach or Security Incident, and measures to be taken to prevent the recurrence or further Disclosure of data regarding such Breach or Security Incident.

d. Notification to Individuals: If notification to individuals whose information was Breached is required under state or federal law, and regardless of whether Recipient is considered only a custodian and/or non-owner of the CIDG Data, Recipient shall, at its sole expense, and at the sole election of CDPH, either:

i. make notification to the individuals affected by the Breach (including substitute notification), pursuant to the content and timeliness provisions of such applicable state or federal Breach notice laws. Recipient shall inform the CDPH Privacy Officer of the time, manner, and content of any such notifications, prior to the transmission of such notifications to the individuals; or

ii. cooperate with and assist CDPH in its notification (including substitute notification) to the individuals affected by the Breach.

e. Submission of Sample Notification to Attorney General: If notification to more than 500 individuals is required pursuant to Civil Code section 1798.29, and regardless of whether Recipient is considered only a custodian and/or non-owner of the CIDG Data, Recipient shall, at its sole expense, and at the sole election of CDPH, either:

i. electronically submit a single sample copy of the security Breach notification, excluding any personally identifiable information, to the Attorney General pursuant to the format, content and timeliness provisions of section 1798.29, subdivision (e). Recipient shall inform the CDPH Privacy Officer of the time, manner, and content of any such submissions, prior to the transmission of such submissions to the Attorney General; or

ii. cooperate with and assist CDPH in its submission of a sample copy of the notification to the Attorney General.

f. Public Statements: Recipient shall cooperate with CDPH in developing content for any public statements regarding Breaches or Security Incidents related to Recipient and shall not provide any public statements without the express written permission of CDPH. Requests for public statement(s) by any non-party about a Breach or Security Incidents shall be directed to the CDPH Program Manager, the CDPH Privacy Officer, and the CDPH Chief Information Security Officer, using the contact information listed in Section XIII(g).

g. CDPH Contact Information: To direct communications to the above referenced CDPH staff, Recipient shall initiate contact as indicated herein. CDPH reserves the right to make

changes to the contact information below by verbal or written notice to Recipient. Said changes shall not require an amendment to this Agreement.

CDPH Program Contract Manager	CDPH Privacy Officer	CDPH Chief Information Security Officer and CDPH IT Service Desk
Shannon Peterson CID Data Strategy Project Manager Center for Infectious Diseases 850 Marina Bay Pkwy, MS7366 Richmond CA, 94806 Email: Shannon.Peterson@cdph.ca.gov	**Privacy Officer** Privacy Office c/o Office of Legal Services California Dept. of Public Health P.O. Box 997377, MS 0506 Sacramento, CA 95899-7377 Email: privacy@cdph.ca.gov Telephone: (877) 421-9634	**Chief Information Security Officer** Information Security Office California Dept. of Public Health P.O. Box 997413, MS 6300 Sacramento, CA 95899-7413 Email: cdph.infosecurityoffice@cdph.ca.gov Telephone: (800) 500-0016

XIV. CDPH Breach and Security Incident Responsibilities: CDPH shall notify Recipient immediately by telephone call and email upon the discovery of a Breach or within twenty-four (24) hours by email of the discovery of any Security Incident that involves data that was created or collected by Recipient into one of the systems set forth in the Exhibits. Notification shall be provided by CDPH to the Recipient Representative, using the contact information listed in the applicable Exhibit. For purposes of this Section, Breaches and Security Incidents shall be treated as discovered by CDPH as of the first day on which such Breach or Security Incident is known to CDPH, or, by exercising reasonable diligence would have been known to CDPH. CDPH shall be deemed to have knowledge of a Breach or Security Incident if such Breach or Security Incident is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach or Security Incident, who is a Workforce Member or agent of CDPH.

XV. Recipient Contact Information: To direct communications to the Recipient's Breach/Security Incident response staff, CDPH shall initiate contact as indicated by Recipient in the applicable Exhibit. Recipient's contact information must be provided to CDPH prior to execution of this Agreement. Recipient reserves theright to make changes to the contact information in the Exhibits. Said changes shall not require an amendment to this Agreement or the Exhibit.

XVI. Compliance with California Health and Safety Code Section 121022(h): CDPH and Recipient shall comply, when required, with California Health and Safety Code section 121022, subdivision (h), which provides as follows: "Any potential or actual breach of confidentiality of HIV-related public health records shall be investigated by the local health officer, in coordination with the department, when appropriate. The local health officer shall immediately report any evidence of an actual breach of confidentiality of HIV-related public health records at a city or county level to the department and the appropriate law enforcement agency. The department shall investigate any potential or actual breach of confidentiality of HIV-related public health records at the state level and shall report any evidence of such a breach of confidentiality to an appropriate law enforcement agency."

XVII. Documentation of Disclosures for Requests for Accounting: Recipient shall document and make available to CDPH or (at the direction of CDPH) to an individual such Disclosures of CIDG Data, and information related to such Disclosures, necessary to respond to a proper request by the subject individual for an accounting of Disclosures of Personal Information as required by Civil Code section 1798.25, or any applicable state or federal law.

XVIII. Requests for CIDG Data by Third Parties: Recipient and its Workforce Member(s), agents, or subcontractors shall promptly transmit to the CDPH Program Contract Manager all requests for Disclosure of any CIDG Data for purposes outside of those permitted under this Agreement or the attached Exhibits requested by third parties to the Agreement between Recipient and CDPH (except from an individual for an accounting of Disclosures of the individual's Personal Information pursuant to applicable state or federal law), unless prohibited from doing so by applicable state or federal law.

XIX. Audits, Inspection and Enforcement: CDPH may inspect the facilities, systems, books, and records of Recipient to monitor compliance with this Agreement. Recipient shall promptly remedy any violation of any provision of this Agreement and shall certify the same to the CDPH Program Contract Manager in writing.

XX. Indemnification: Each Party hereby agrees that CIDG Data collected by Recipients in all CDPH databases is collected for the mutual benefit of the counties and the state under applicable state and local health department authority HSC § 120130 et seq. and 17 California Code of Regulations section 2500 et seq., which designate what reportable diseases, conditions and fields are to be Used to collect information. With this understanding, all Parties agree to indemnify, hold harmless, and defend the other Party from and against any and all claims, losses, liabilities, damages, costs and other expenses (including attorneys' fees) that result from or arise directly or indirectly out of or in connection with any negligent act or omission or willful misconduct of Recipient or CDPH, its officers, Workforce Member(s), or agents relative to the CIDG Data, including, without limitation, any violations of Recipient's or CDPH's responsibilities under this Agreement. This mutual indemnification is intended to include current or future system's collection of CIDG Data in any CDPH database as deemed necessary for inclusion by mutual agreement between CDPH and Recipient through a written agreement. This separate agreement will be provided by CDPH to Recipient, once future systems are available for use and consideration, which will need to be mutually agreed upon and fully executed prior to access. Any new and separate agreements executed by the Parties will be attached to this master Agreement in the same manner as the current data system exhibits. Should a Breach or Security Incident occur, the Parties understand that their obligations under the individual data system exhibits, attached to this master agreement, along with the clauses herein referencing all notifications, investigations, written reports and public statements, shall be enforced in accordance with those exhibits.

XXI. Term of Agreement: Unless otherwise terminated earlier in accordance with the provisions set forth herein, this Agreement shall remain in effect for three (3) years after the latest signature date in the signature block below. After three (3) years, this Agreement will expire without further action. If the Parties wish to extend this Agreement, they may do so by reviewing, updating, and reauthorizing this Agreement via a written amendment signed by both Parties. If one or both Parties wish to terminate this Agreement prematurely, they may do so without cause and for any reason upon thirty (30) days advanced notice. CDPH may also terminate this Agreement pursuant to Section XXII, below.

XXII. Termination for Cause:

a. Termination Upon Material Breach: A violation by Recipient of any provision of this Agreement, as determined by CDPH, shall constitute a material breach of the Agreement and grounds for immediate termination of the Agreement by CDPH. At its sole discretion, CDPH may give Recipient thirty (30) days to cure the breach.

b. Judicial or Administrative Proceedings: Recipient will notify CDPH if it is named as a defendant in a criminal proceeding related to a violation of this Agreement. CDPH may immediately terminate the Agreement if Recipient is found guilty of a criminal violation related to a violation of this Agreement. CDPH may terminate the Agreement if a finding or stipulation that Recipient has violated any security or privacy laws is made in any administrative or civil proceeding in which Recipient is a party or has been joined.

XXIII. Amendment: The Parties acknowledge that federal and state laws regarding information security and privacy rapidly evolve and that amendment of this Agreement may be required to provide for procedures to ensure compliance with such laws. The Parties specifically agree to take such action as is necessary to implement new standards and requirements imposed by regulations and other applicable laws relating to the security or privacy of CIDG Data. The Parties agree to promptly enter into negotiations concerning an amendment to this Agreement consistent with new standards and requirements imposed by applicable laws and regulations.

XXIV. Assistance in Litigation or Administrative Proceedings: Recipient shall make itself and any Workforce Member(s) assisting Recipient in the performance of its obligations under the Agreement between Recipient and CDPH, available to CDPH at no cost to CDPH to testify as witnesses, in the event of litigation or administrative proceedings being commenced against CDPH, its director, officers or employees based upon claimed violation of laws relating to security and privacy, which involves inactions or actions by Recipient, except where Recipient or its or its Workforce Member(s) is a named adverse party.

XXV. Disclaimer: CDPH makes no warranty or representation that compliance by Recipient with this Agreement or the Exhibits will be adequate or satisfactory for Recipient's own purposes or that any information in Recipient's possession or control, or transmitted or received by Recipient, is or will be secure from unauthorized Use or Disclosure. Recipient is solely responsible for all decisions made by Recipient regarding the safeguarding of CIDG Data.

XXVI. No Third-Party Beneficiaries: Nothing express or implied in the terms and conditions of this Agreement is intended to confer, nor shall anything herein confer, upon any person other than CDPH or Recipient and their respective successors or assignees, any rights, remedies, obligations, or liabilities whatsoever.

XXVII. Assignment: No assignment of this Agreement or of the rights and obligations hereunder shall be valid without the prior written consent of the other Party.

XXVIII. Waiver: No delay or failure to perform any provision of this Agreement shall constitute a waiver of that provision as to that or any other instance. Any waiver granted by a party shall be in writing and shall apply to the specific instance expressly stated.

XXIX. Interpretation: The terms and conditions in this Agreement shall be interpreted as broadly as necessary to implement and comply with regulations and applicable state laws. The Parties agree that any ambiguity in the terms and conditions of this Agreement shall be resolved in favor of a meaning that complies and is consistent with federal and state laws and regulations.

XXX. Survival: If Recipient does not return or destroy the CIDG Data upon the expiration or termination of the Agreement, the respective rights and obligations of Recipient under Sections VIII, IX, XIII, and XX of this Agreement shall survive the expiration or termination of the Agreement between Recipient and CDPH.

XXXI. Entire Agreement: This Agreement, including all Exhibits as referenced herein, constitute the entire agreement between CDPH and Recipient. Any modifications of this Agreement must be in writing and signed by all Parties. Any oral representations or agreements between the Parties shall be of no force or effect.

XXXII. Severability: The invalidity in whole or in part of any provisions of this Agreement shall not void or affect the validity of any other provisions of this Agreement.

XXXIII. Choice of Law: This Agreement shall be governed, construed and enforced in accordance with the laws of the State of California, excluding choice of law principles. All disputes with respect to this Agreement shall be brought and heard exclusively either in the California state or federal courts. The parties to this Agreement each consent to the *in personam* jurisdiction and venue of such courts exclusively.

XXXIV. Electronic Signatures: This Agreement may be executed in any number of counterparts, each of which so executed shall be deemed to be an original, and such counterparts shall together constitute one and the same Agreement. The parties shall be entitled to sign and transmit an electronic signature of this Agreement (whether by facsimile, PDF or other mail transmission), which signature shall be binding on the party whose name is contained therein.

XXXV. Signatures:

IN WITNESS, WHEREOF, the Parties have executed this Agreement as follows:

On behalf of Recipient, the undersigned individual hereby attests that they are authorized to enter into this Agreement and agrees to abide by and enforce all the terms specified herein.

Sharon Wang, DO, MSHPE, FIDSA Name (Print)	_____ Name (Sign)
Health Officer Title [Health Officer (or other authorized official)]	_____ Date
San Bernardino County Department of Public Health County/City Name (Print)	

On behalf of CDPH, the undersigned individual hereby attests that they are authorized to enter into this Agreement and agrees to all the terms specified herein.

_____	_____
James Watt, M.D., M.P.H. Chief, Division of Communicable Disease Control California Department of Public Health	Date

Exhibit A – California Connected

California CONNECTED (hereinafter referred to as CalCONNECT) (includes both the CalCONNECT Transactional System and the CalCONNECT Data Warehouse) (hereinafter referenced as the CalCONNECT System) Exhibit, in conjunction with the Center for Infectious Diseases General Data Use and Disclosure Agreement (Agreement) sets forth the requirements CDPH and Recipient are obligated to follow. with respect to all CalCONNECT Data (as defined herein) Permission to collect, receive, use, and disclose CalCONNECT Data requires Recipient to agree to the Agreement and this Exhibit and all terms, conditions, and limitations of Recipient's collection, use, and disclosure of the CalCONNECT Data.

I. Background and Purpose: The CalCONNECT System is an online database that maintains information, originally collected by local health departments, CDPH, or their agents, related to Contagious, Infectious, Communicable or Reportable Diseases and Conditions (CICR Diseases and Conditions). It was initially established in response to the 2020 worldwide outbreak of COVID-19 to aid CDPH to take measures as necessary to ascertain the nature of the disease and prevent its spread; and has since been expanded for use to collect information on any CICR Diseases and Conditions. The purpose of this database is to improve the efficiency of disease surveillance and response activities and the early detection of public health events through the collection of more complete and timely surveillance information on a state-wide basis. CalCONNECT is a secure, web-based electronic solution for Recipient and CDPH to maintain information from interviews with cases and contacts, which identify the individuals they have interacted with, collect their conditions and symptoms, and notify those contacts to evaluate whether they need to isolate or quarantine or whether any additional measures or medical treatment are necessary or appropriate. CalCONNECT is a system managed by CDPH and used by Recipient for surveillance, control and coordination of medical services related to Contagious, Infectious, Communicable or Reportable Diseases and Conditions, which is accomplished by pulling pertinent information about an individual from other CDPH databases like CAIR and CalREDIE. The CalCONNECT Datawarehouse is an online database that stores information originally collected by local health departments, CDPH, or their agents, related to a CICRDC that permits local health departments to evaluate and assess how a specific CICRDC is affecting their jurisdiction and to assist them with providing timely measures to prevent the further spread of any disease.

II. Definitions: For purposes of this Exhibit, the following definitions shall apply in addition to those set forth in the Agreement:

A. CalCONNECT Data: "CalCONNECT Data" means data in the CalCONNECT Transactional state-wide reportable disease database and CalCONNECT Data Warehouse supported and maintained by CDPH including demographic, epidemiologic (including clinical information, risk factor information, and laboratory test result information), as well as administrative information on Contagious, Infectious, Communicable or Reportable Diseases and Conditions collected for contact tracing, case investigation, and for examining the causes of the communicable diseases and conditions, to ascertain the nature of the disease or condition and to prevent its spread.

1. CalCONNECT Data specifically includes information contained in or derived from the following:

a. Confidential Morbidity Report (CMR) required by Title 17 of the California Code of Regulations (CCR) sections 2500, 2593, 2641.5-2643.20, and 2800-2812 Reportable Diseases and Conditions.

b. Laboratory Test and Result information required by Title 17 of the CCR sections 2505 and 2641.5 - 2643.20.

c. Communicable Disease Control Report Forms (required for specific diseases and conditions that are mandated by state laws and regulations to be reported by healthcare providers and laboratories to local health officers), including cases of the Contagious, Infectious, Communicable or Reportable Diseases and Conditions along with related immunization data.

2. CalCONNECT Activities may include the collection of:

a. Demographic data of cases and contacts;

b. Information obtained through interviews with cases and contacts, including but not limited to, self-reported health information, long term symptoms, demographic information, location and location history information, risk factor information, laboratory test results, and other personal information as defined by Civil Code section 1798.3; and

c. Records of communications with cases and contacts, which contain personal information as defined by Civil Code section 1798.3, including but not limited to, phone call recordings, SMS (text) messages, call logs, and tracking sheets.

3. CalCONNECT Data specifically excludes the following information:

Mental health information unrelated to the Contagious, Infectious, Communicable or Reportable Diseases and Conditions being monitored.
Substance user disorder information provided by any 42 CFR Part 2 federally assisted program provider for the treatment of substance use disorders.
Health information for any minor under the age of 12 wherein parental consent has not been properly and legally obtained by the LHJ.
California Supplemental Pay Sick Leave (“CSPSL”) aka “Backpay”
Religious beliefs, practices or observances which include moral or ethical beliefs and
Political, sociological or philosophical views affiliated with any individual.

III. Legal Authority for Collection, Use and Disclosure of CalCONNECT Data: The legal authority for CDPH and Recipient to collect, use and disclose CalCONNECT Data include the following:

1. California Civil Code section 1798.24(i)
2. California Health and Safety Code section 101085
3. California Health and Safety Code section 120125
4. California Health and Safety Code section 120130
5. California Health and Safety Code section 120140
6. California Health and Safety Code sections 120175 & 120175.5
7. California Health and Safety Code sections 120500-120605
8. California Health and Safety Code sections 120975-121023
9. California Health and Safety Code sections 121025-121035
10. Title 17 Public Health, Division 1. State Department of Health Services, Chapter 4. Preventative Medical Service, Article 1, Reporting Sections:2500, and 2505
11. Title 17. Public Health, Division 1. State Department of Health Services, Chapter 4. Preventative Medical Service, Article 3.5, Reporting of HIV, Sub Article 4, Sections: 2641.5-2643.20

IV. Permitted Disclosures: Recipient acknowledges that once data is entered into the CalCONNECT system, Recipient and its Workforce Members and agents, shall safeguard the CalCONNECT Data to which they have access to from unauthorized disclosure. Recipient, and its Workforce Members and agents, shall

not disclose any CalCONNECT Data for any purpose other than carrying out the Recipient's obligations under the statutes and regulations set forth in this Exhibit, or as otherwise allowed or required by state or federal law. When cases and contacts cross into another county's jurisdiction, Recipient is permitted to disclose CalCONNECT Data with the local health department of that county's jurisdiction. Any such disclosure of CalCONNECT Data shall be limited to the minimum necessary, to the extent practicable, in carrying out Recipient's obligations under this Exhibit or as otherwise allowed or required by state or federal law. Requests for release of data through generated reports created by CDPH will be disclosed to Recipient when permissible. Otherwise, Recipient acknowledges the necessity of safeguarding the CalCONNECT Data in accordance with state and federal laws. Should unauthorized disclosures of CalCONNECT Data be confirmed by CDPH or the Recipient regarding one of its Workforce Members and agents, immediate access to the individual will be removed. All requests to reinstate the individual for access in the future will need to be made on a case-by-case basis to the CDPH Privacy Office for further consideration. Recipient also acknowledges that Syphilis Summary Reports and Tuberculosis Summary Reports may be pulled by CDPH from data collected by various counties throughout the State of California which may contain medical records regarding lab history, prior treatment, and diagnosis for an individual that extends beyond the scope of the current jurisdiction in which an individual may reside.

V. Permitted Use: Recipient, and its Workforce Members and agents, shall safeguard the CalCONNECT Data to which they have access from unauthorized use. Recipient, and its Workforce Members and agents, shall not use any CalCONNECT Data for any purpose other than carrying out Recipient's obligations under the laws and regulations set forth in this Exhibit or as otherwise allowed or required by state or federal law. Should unauthorized use of CalCONNECT Data be confirmed by CDPH or the Recipient regarding one of its Workforce Members and agents, immediate access to the individual will be removed. All requests to reinstate the individual for access in the future will need to be made on a case by case basis to the CDPH Privacy Office for further consideration.

VI. Mandated Training: Recipient, shall ensure that all its Workforce Members and agents, have completed the mandatory trainings issued by CDPH on the proper handling of all CalCONNECT System Data prior to accessing the CalCONNECT Transactional System and the CalCONNECT Data Warehouse. Certifications of completion will continue to be issued by CDPH to Recipient Workforce Members and agents upon completion and Recipient should have all certifications available for review and confirmation of completion, if deemed necessary. Annual training will be required for each individual accessing the CalCONNECT System.

VII. Restricted Disclosures and Uses: Recipient shall limit the access it provides to its Workforce Members and agents to the minimum necessary. Additionally, should Recipient determine a Workforce Member's duties require access to any CalREDIE or CalCONNECT Data related to HIV, Recipient is responsible for instructing the Workforce Member as to their responsibilities under the law. Recipient will have the Workforce Member sign the HIV Confidentiality Acknowledgement and then maintain a copy of the Acknowledgement in the Recipient's records, as well as provide a copy of the Acknowledgement to CDPH. Any other use is strictly prohibited. Any such use of CalCONNECT Data shall be limited to the minimum necessary, to the extent practicable, in carrying out the Recipient's obligations under this Agreement or as otherwise allowed or required by state or federal law. Participant shall collect no more than the minimum amount of information necessary to perform its obligations as set forth in this Agreement. Further, should the Participant collect any CalCONNECT Data that may be protected by 42 CFR Part 2, a federal regulation that requires substance abuse disorder treatment providers to observe additional privacy and confidentiality restrictions with respect to patient records in the CalCONNECT system, they must adhere to those stringent privacy protections which are more restrictive than HIPAA. Any and all violations may be grounds for removal from use of CalCONNECT at the election of CDPH.

VIII. Disclaimer: CDPH makes no warranty or representation that compliance by Recipient with this Exhibit will be adequate or satisfactory for Recipient's own purposes or that any information in Recipient's possession or control, or transmitted or received by Recipient, is or will be secure from unauthorized use or disclosure. Recipient is solely responsible for all decisions made by Recipient regarding the safeguarding of CalCONNECT Data.

IX. Contact Information: To direct communications to the other party regarding this Exhibit, CDPH or Recipient shall use the contact information below. The Parties reserve the right to make changes to the contact information below by verbal or written notice. Changes do not require an amendment to this Agreement.

CDPH Program Data Systems Manager	**CDPH Privacy Officer**	**CDPH Chief Information Security Officer and CDPH IT Service Desk**
Ryan Murphy, PhD MPH Branch Chief, CalCONNECT Branch, Division of Communicable Disease Control, Center for Infectious Diseases, California Department of Public Health Email: Ryan.Murphy@cdph.ca.gov Phone: (510)-620-6718	**Privacy Officer** Privacy Office c/o Office of Legal Services California Dept. of Public Health P.O. Box 997377, MS 0506 Sacramento, CA 95899-7377 Email: privacy@cdph.ca.gov Telephone: (877) 421-9634	**Chief Information Security Officer** Information Security Office California Dept. of Public Health P.O. Box 997413, MS 6300 Sacramento, CA 95899-7413 Email: cdph.infosecurityoffice@cdph.ca.gov Telephone: (800) 500-0016
Recipient Program Manager	**Recipient Privacy Officer**	**Recipient Information Security Officer**

Exhibit B – California Immunization Registry

This California Immunization Registry (CAIR) Exhibit in conjunction with the Center for Infectious Diseases General Data Use and Disclosure Agreement (Agreement) sets forth the requirements CDPH and Recipient are obligated to follow with respect to all CAIR Data (as defined herein) collected or created within CAIR. In order to access, view, add, and/or modify immunization information and/or tuberculosis (TB) test results in CAIR, Recipient agrees to all terms, conditions, and limitations of Recipient's collection, use, and disclosure of the CAIR Data as set forth in the Agreement and this Exhibit.

I. Background and Purpose: CAIR2 is a secure, confidential, computerized online statewide information immunization system (IIS) managed by the Immunization Branch of CDPH's Center for Infectious Diseases. It was developed to assist local health jurisdictions and other approved organizations/entities to track and review immunization information and TB test results for individuals, assess immunization needs and remind/recall patients, avoid unnecessary or redundant immunizations, and control disease outbreaks. Providers in most counties report vaccination data directly to CAIR2; providers in the other counties report data to the Healthy Futures IIS, which in turn exchanges data with CAIR2. Collectively the two IIS are referred to as CAIR. Information in CAIR is only available to authorized users.

II. Definitions: For purposes of this Exhibit, the following definitions shall apply in addition to those set forth in the Agreement:

A. California Immunization Registry (CAIR) Data: "CAIR Data" means data uploaded to CAIR2 and Health Futures IIS pursuant to Health and Safety Code (HSC) § 120440(c), which is maintained in the statewide IIS referred to as CAIR supported and maintained by CDPH's Immunization Branch.

III. Legal Authority for Collection, Use and Disclosure of CAIR Data: The legal authority for CDPH and Recipient to collect, use and disclose CAIR Data include the following:

1. California Civil Code § 1798.24(e)
2. California HSC § 120440

IV. Permitted Use and Disclosures: Recipient and its Workforce Members and agents, shall safeguard the CAIR Data to which they have access from unauthorized disclosure. Recipient, and its Workforce Members and agents, shall not disclose any CAIR Data for any purpose other than carrying out the Recipient's obligations under the statutes and regulations set forth in this Exhibit, or as otherwise allowed or required by state or federal law.

V. Restricted Disclosures and Uses: Recipient shall limit the access it provides to its workforce members and agents to the minimum necessary. Additionally, should an individual exercise their rights to refuse to permit record sharing under HSC § 120440(e), Recipient may only maintain access to the information for the purpose of protecting the public health.

VI. Disclaimer: CDPH makes no warranty or representation that compliance by Recipient with this Agreement or Exhibit will be adequate or satisfactory for Recipient's own purposes or that any information in Recipient's possession or control, or transmitted or received by Recipient, is or will be secure from unauthorized use or disclosure. Recipient is solely responsible for all decisions made by Recipient regarding the safeguarding of CAIR Data.

VII. Contact Information: To direct communications to the other party regarding this Exhibit, CDPH or Recipient shall use the contact information below. The Parties reserve the right to make changes to the

contact information below by verbal or written notice. Changes do not require an amendment to this Agreement.

CDPH Program Manager	**CDPH Privacy Officer**	**CDPH Chief Information Security Officer and CDPH IT Service Desk**
Michael S. Powell, MSc., Chief Registry & Assessments Sect. Div. of Communicable Disease Control Center for Infectious Diseases Ca. Dept. of Public Health Email: Michael.Powell@cdph.ca.gov Telephone: (279) 667-0121	**Privacy Officer** Privacy Office c/o Office of Legal Services California Dept. of Public Health P.O. Box 997377, MS 0506 Sacramento, CA 95899-7377 Email: privacy@cdph.ca.gov Telephone: (877) 421-9634	**Chief Information Security Officer** Information Security Office California Dept. of Public Health P.O. Box 997413, MS 6300 Sacramento, CA 95899-7413 Email: cdph.infosecurityoffice@cdph.ca.gov Telephone: (800) 500-0016
Recipient Program Manager	**Recipient Privacy Officer**	**Recipient Information Security Officer**

Exhibit C – California Reportable Disease Information Exchange (CalREDIE)

This California Reportable Disease Information Exchange (**CalREDIE**) Exhibit, in conjunction with the Center for Infectious Diseases General Data Use and Disclosure Agreement (Agreement) sets forth the requirements CDPH and Recipient are obligated to follow with respect to all CalREDIE Data (as defined herein) collected or created within CalREDIE. Permission to collect, receive, use, and disclose CalREDIE Data requires Recipient to agree to the Agreement and this Exhibit and all terms, conditions, and limitations of Recipient's collection, use, and disclosure of the CalREDIE Data.

I. Background and Purpose: CalREDIE is a system of applications that encompasses the core surveillance and reporting application, electronic laboratory reporting (ELR) application, ELR message handling application, provider reporting application, alerting and notification application, Data Warehouse (DW), and Data Distribution Portal (DDP) that CDPH has implemented for web-based disease reporting and surveillance. The purpose of CalREDIE is to improve the efficiency of surveillance activities and the early detection of public health events through the collection of more complete and timely surveillance information on a statewide basis. CalREDIE is a secure, web-based electronic solution for health care providers to report cases of conditions of public health interest; and for laboratories to report laboratory reports for notifiable conditions to LHDs and CDPH, and for LHDs to report conditions to CDPH. CalREDIE is an integral part of the overall California public health emergency preparedness and response strategy and use of CalREDIE allows for 24/7/365 reporting and receipt of notifiable conditions. LHDs and CDPH have access to disease and laboratory reports in near real-time for disease surveillance, public health investigation, and case management activities. CalREDIE is the system of record for communicable disease surveillance data within California.

II. Definitions: For purposes of this Exhibit, the following definitions shall apply in addition to those set forth in the Agreement:

A. CalREDIE Data: "CalREDIE Data" means data in the state-wide reportable disease database supported and maintained by CDPH including demographic, epidemiologic (including clinical information, risk factor information, and laboratory test result information), and administrative information on reportable diseases collected for the purposes of case investigation, disease prevention, and surveillance.

1. CalREDIE Data specifically includes information contained in or derived from the following:

a. Confidential Morbidity Report (CMR) required by Title 17 of the California Code of Regulations (CCR) sections 2500, 2593, 2641.5-2643.20, and 2800-2812 Reportable Diseases and Conditions.

b. Laboratory Test and Result information required by Title 17 of the CCR sections 2505 and 2641.5 - 2643.20.

c. Communicable Disease Control Report Forms (obtained from healthcare providers, laboratories, and local health departments pursuant to state and federal law including but not limited to Title 17 CCR sections 2500 et seq.)

B. Designated Users: "Designated Users" means individuals from Recipient's jurisdiction granted a read-only user account with permissions to access the Shared Disease Grouping and Shared Jurisdiction Grouping. Designated Users are only permitted read-only access to both Recipient's data and the data from other participating jurisdictions. Each Recipient may designate up to three (3) individuals as Designated Users.

III. Legal Authority for Collection, Use and Disclosure of CalREDIE Data: The legal authority for CDPH and Recipient to collect, use and disclose CalREDIE Data include the following:

1. California Civil Code section 1798.24(e);
2. Title 17 California Code of Regulations section 2500, et. seq.

IV. Permitted Uses and Disclosures: Recipient and its Designated Users shall safeguard the CalREDIE Data to which they have access to from unauthorized use and disclosure. Recipient, and its Designated Users, shall not use or disclose any CalREDIE Data for any purpose other than carrying out the Recipient's obligations under the statutes and regulations set forth in this Exhibit, or as otherwise allowed or required by state or federal law.

V. Restricted Disclosures and Uses: Recipient shall limit the access it provides to its Designated Users to the minimum necessary. Additionally, should the Recipient determine a Designated User's duties require access to any CalREDIE Data related to HIV, Recipient is responsible for instructing the Designated User as to their responsibilities under the law. Recipient will have the Designated User sign the HIV Confidentiality Acknowledgement and then maintain a copy of the Acknowledgement in the Recipient's records, as well as provide a copy of the Acknowledgement to CDPH.

VI. Disclaimer: CDPH makes no warranty or representation that data provided to Recipient pursuant to its compliance with this Exhibit will be adequate or satisfactory for Recipient's own purposes or that any information in Recipient's possession or control, or transmitted or received by Recipient, is or will be secure from unauthorized use or disclosure. Recipient is solely responsible for all decisions made by Recipient regarding the safeguarding of CalREDIE Data.

VII. Contact Information: To direct communications to the other party regarding this Exhibit, CDPH or Recipient shall use the contact information below. The Parties reserve the right to make changes to the contact information below by verbal or written notice. Changes do not require an amendment to this Exhibit.

[CONTINUED ON NEXT PAGE]

CDPH Program Manager	CDPH Privacy Officer	CDPH Chief Information Security Officer and CDPH IT Service Desk
Abigail Kroch, PhD MPH Branch Chief, Public Health Reporting Information Exchange (PRIME) Division of Communicable Disease Control California Department of Public Health Phone: 916.720.8268 Abigail.Kroch@cdph.ca.gov	**Privacy Officer** Privacy Office c/o Office of Legal Services California Dept. of Public Health P.O. Box 997377, MS 0506 Sacramento, CA 95899-7377 Email: privacy@cdph.ca.gov Telephone: (877) 421-9634	**Chief Information Security Officer** Information Security Office California Dept. of Public Health P.O. Box 997413, MS 6300 Sacramento, CA 95899-7413 Email: cdph.infosecurityoffice@cdph.ca.gov Telephone: (800) 500-0016
Recipient Program Manager	**Recipient Privacy Officer**	**Recipient Information Security Officer**

Exhibit D – California Integrated Infectious Disease Data Warehouse

This California Integrated Infectious Disease Data Warehouse (I2D2) Exhibit in conjunction with the Center for Infectious Diseases General Data Use and Disclosure Agreement (Agreement) sets forth the requirements CDPH and Recipient are obligated to follow with respect to all I2D2 Data (as defined herein) maintained within I2D2. In order to access, view, add, and/or modify I2D2 Data, Recipient agrees to all terms, conditions, and limitations of Recipient's access, use, and disclosure of the I2D2 Data as set forth in the Agreement and this Exhibit.

I. Background and Purpose: I2D2 centralizes, transforms, and shares data from state and local disease reporting systems so they are aligned and standardized yielding a statewide infectious disease data resource. This means all infectious disease data analyses, analytic models, dashboards, and reports can be sourced from the same data source. A single centralized dataset also enables centralized data quality control and data processing so corrections and improvements can be applied and deployed in one place at one time, significantly reducing effort and complications for data users. This is especially beneficial for Recipients with limited data analysis capacity. Epidemiologists and modelers mostly access the data via an Open Database Connectivity (ODBC) connection with Snowflake. Some users also use the Snowflake web interface for analysis. Access to I2D2 by Recipient staff is intended to increase scalability and standardization of infectious disease monitoring, accessibility regardless of a user's skillset, automation of data usage, collaboration between users, and efficiency of reporting. Additionally, it will provide a single source for analysis, dashboards, and reports.

II. Definitions: For purposes of this Exhibit, the following definitions shall apply in addition to those set forth in the Agreement:

A. California Immunization Registry (CAIR): "CAIR" means data uploaded to CAIR2 and Health Futures IIS pursuant to Health and Safety Code (HSC) § 120440(c), which is maintained in the statewide IIS referred to as CAIR supported and maintained by CDPH's Immunization Branch.

B. California Reportable Disease Information Exchange (CalREDIE): "CalREDIE" means data in the statewide reportable disease database supported and maintained by CDPH including demographic, epidemiologic (including clinical information, risk factor information, and laboratory test result information), and administrative information on reportable diseases collected for the purposes of case investigation, disease prevention, and surveillance.

1. CalREDIE Data specifically includes information contained in or derived from the following:

a. Confidential Morbidity Report (CMR) required by Title 17 of the California Code of Regulations (CCR) sections 2500, 2593, 2641.5-2643.20, and 2800-2812 Reportable Diseases and Conditions.

b. Laboratory Test and Result information required by Title 17 of the CCR sections 2505 and 2641.5 - 2643.20.

c. Communicable Disease Control Report Forms (required for specific diseases and conditions that are mandated by state law and regulations to be reported by healthcare providers and laboratories to local health officers.

C. I2D2 Data: "I2D2 Data" means the data maintained in I2D2, which is derived from CAIR, CalREDIE, IRIS, NHSN, WebCMR, SaPHIRE, WSS, Kaiser NorCath, and VR (as those systems are defined herein).

D. Los Angeles County Integrated Reporting, Investigation, and Surveillance (IRIS) system: "IRIS" means the electronic reporting system for communicable diseases. Its main purpose is to make disease reporting, investigation, and tracking more efficient for Disease Control Programs in Los Angeles County. IRIS contains information for the full investigative cycle of a disease or outbreak from date of onset to the final resolution.

E. National Healthcare Safety Network (NHSN): "NHSN" means the Center for Disease Control's healthcare-associated infection tracking system. Specifically, for the purposes of this Exhibit, it refers only to HNSN's aggregated hospitalization data for COVID, Flu, and RSV.

F. San Diego County WebCMR (WebCMR): "WebCMR" means the communicable disease registry system maintained by San Diego County, which supports public health disease surveillance and investigation. It is linked to an electronic laboratory reporting system, which allows laboratories to electronically send public health reports that identify conditions that are notifiable.

G. Surveillance and Public Health Information Reporting and Exchange – Testing Observations Results Exchange ("SaPHIRE-TORX"): "SaPHIRE-TORX" means the electronic lab result data and electronic initial case report for COVID.

H. Wastewater Sewer Shed (WSS): "WSS" means the wastewater sewer shed facility meta data for de-identified sewer specimen sample information.

I. Kaiser NorCath: Kaiser NorCath is aggregate de-identified hospitalization data for respiratory viruses.

J. Vital Records (VR): "VR" means the non-confidential portion of birth, death, and fetal death certificates.

III. Legal Authority for Collection, Use and Disclosure of I2D2 Data: The legal authority for CDPH and Recipient to use I2D2 Data include the following:

1. CA Civil Code § 1798.24(e)
2. CA HSC § 120125
3. CA HSC § 120130
4. CA HSC § 120140
5. CA HSC § 120185
6. CA HSC § 120190
7. CA CCR Title 17 § 2500
8. CA CCR § 2502
9. CA CCR § 2505

IV. Permitted Use and Disclosures: Recipient and its Workforce Members and agents, shall safeguard the I2D2 Data to which they have access from unauthorized disclosure. Recipient, and its Workforce Members and agents, shall not disclose any I2D2 Data for any purpose other than carrying out the Recipient's obligations under the statutes and regulations set forth in this Exhibit, or as otherwise allowed or required by state or federal law.

V. Restricted Disclosures and Uses: Recipient shall limit the access it provides to its Workforce Member(s) and agents to the minimum necessary.

VI. Disclaimer: CDPH makes no warranty or representation that compliance by Recipient with this Agreement or Exhibit will be adequate or satisfactory for Recipient's own purposes or that any information in Recipient's possession or control, or transmitted or received by Recipient, is or will be secure from unauthorized use or disclosure. Recipient is solely responsible for all decisions made by Recipient regarding the safeguarding of I2D2 Data.

VII. Training: Recipient is responsible for assuring all of its Workforce Members granted access to I2D2 Data will have completed all training CDPH requires a user to complete in order to access the data in its original system.

VIII. HIV Confidentiality Statement: Recipient is responsible for assuring all of its Workforce Members who may access confidential HIV-related public health records have signed the CDPH Office of AIDS' Confidentiality Agreement. This requirement applies regardless of whether the access is an essential or incidental part of their work.

IX. Contact Information: To direct communications to the other party regarding this Exhibit, CDPH or Recipient shall use the contact information below. The Parties reserve the right to make changes to the contact information below by verbal or written notice. Changes do not require an amendment to this Agreement.

CDPH Program Manager	**CDPH Privacy Officer**	**CDPH Chief Information Security Officer and CDPH IT Service Desk**
Emilia Reilly, MPH Acting Branch Chief Informatics Branch Div. Communicable Disease Ctrl. Center for Infectious Disease Ca. Dept. of Public Health Email: Emilia.Reilly2@cdph.ca.gov Telephone: (279) 203-8613	**Privacy Officer** Privacy Office c/o Office of Legal Services CA Dept. of Public Health P.O. Box 997377, MS 0506 Sacramento, CA 95899-7377 Email: privacy@cdph.ca.gov Telephone: (877) 421-9634	**Chief Information Security Officer** Information Security Office California Dept. of Public Health P.O. Box 997413, MS 6300 Sacramento, CA 95899-7413 Email: cdph.infosecurityoffice@cdph.ca.gov Telephone: (800) 500-0016
Recipient Program Manager	**Recipient Privacy Officer**	**Recipient Information Security Officer**

Exhibit E – My Turn

This My Turn Vaccine Management System (My Turn) Exhibit in conjunction with the Center for Infectious Diseases General Data Use and Disclosure Agreement (Agreement) sets forth the requirements CDPH and Recipient are obligated to follow with respect to all My Turn Data (as defined herein) collected or created within My Turn. In order to access, view, add, and/or modify data in My Turn, Recipient agrees to all terms, conditions, and limitations of Recipient's collection, use, and disclosure of the My Turn Data as set forth in the Agreement and this Exhibit.

I. Background and Purpose: My Turn is a secure, web-based platform that 1) connects individuals with tools and resources to schedule appointments and receive vaccinations and 2) provides clinic managers and vaccine administrators an all-in-one application for vaccine eligibility, public appointment scheduling, walk-in appointments, dose administration, and reporting for vaccine clinics. My Turn Clinic is used by Californian Local Health Jurisdictions (LHJs) to manage appointments, clinics, and records, and document the administration of vaccines. My Turn then submits those records to the California Immunization Registry. My Turn was established in response to COVID-19 and, after initial expansion to flu and the mpox vaccine it has now been expanded to include all other common vaccines administered in California.

II. Definitions: For purposes of this Exhibit, the following definitions shall apply in addition to those set forth in the Agreement:

A. My Turn Data: "My Turn Data" means data uploaded to My Turn Public by an individual or My Turn Clinic by an LHJ or Provider. My Turn is maintained by CDPH's Immunization Branch in the Center for Infectious Diseases.

III. Legal Authority for Collection, Use and Disclosure of My Turn Data: The legal authority for CDPH and Recipient to collect, use and disclose My Turn Data include the following:

1. California Civil Code § 1798.24(e)
2. California Health and Safety Code (HSC) § 120175
3. California HSC § 120440
4. California HSC § 131050

IV. Permitted Use and Disclosures: Recipient and its Workforce Members and agents, shall safeguard the My Turn Data to which they have access from unauthorized disclosure. Recipient, and its Workforce Members and agents, shall not disclose any My Turn Data for any purpose other than carrying out the Recipient's obligations under the statutes and regulations set forth in this Exhibit, or as otherwise allowed or required by state or federal law.

V. Restricted Disclosures and Uses: Recipient shall limit the access it provides to its workforce members and agents to the minimum necessary. Additionally, should an individual exercise their rights to refuse to permit record sharing under HSC § 120440(e), Recipient may only maintain access to the information for the purpose of protecting the public health.

VI. Disclaimer: CDPH makes no warranty or representation that compliance by Recipient with this Agreement or Exhibit will be adequate or satisfactory for Recipient's own purposes or that any information in Recipient's possession or control, or transmitted or received by Recipient, is or will be secure from unauthorized use or disclosure. Recipient is solely responsible for all decisions made by Recipient regarding the safeguarding of My Turn Data.

VII. Contact Information: To direct communications to the other party regarding this Exhibit, CDPH or Recipient shall use the contact information below. The Parties reserve the right to make changes to the contact information below by verbal or written notice. Changes do not require an amendment to this Agreement.

CDPH Program Manager	**CDPH Privacy Officer**	**CDPH Chief Information Security Officer and CDPH IT Service Desk**
Michael S. Powell, MSc., Chief Registry & Assessments Sect. Div. of Communicable Disease Control Center for Infectious Diseases Ca. Dept. of Public Health Email: Michael.Powell@cdph.ca.gov Telephone: (279) 667-0121	**Privacy Officer** Privacy Office c/o Office of Legal Services California Dept. of Public Health P.O. Box 997377, MS 0506 Sacramento, CA 95899-7377 Email: privacy@cdph.ca.gov Telephone: (877) 421-9634	**Chief Information Security Officer** Information Security Office California Dept. of Public Health P.O. Box 997413, MS 6300 Sacramento, CA 95899-7413 Email: cdph.infosecurityoffice@cdph.ca.gov Telephone: (800) 500-0016
Recipient Program Manager	**Recipient Privacy Officer**	**Recipient Information Security Officer**

Exhibit F – California Reportable Disease Information Exchange (CalREDIE)
Cross-Jurisdictional Data Sharing

This CalREDIE Cross-Jurisdictional Data Sharing Exhibit, in conjunction with the Center for Infectious Diseases General Data Use and Disclosure Agreement (Agreement) provides guidance to Recipient regarding how CalREDIE Data (as defined herein) can be shared across jurisdictions in an authorized and secure manner.

I. Background and Summary: The implementation of CalREDIE as a tool to support disease surveillance efforts in California has introduced changes and, in general, increased efficiency in how Local Health Jurisdiction (LHJ) staff access and share surveillance data. Restriction of the ability to share surveillance data across jurisdictions limits public health activities. Therefore, CalREDIE includes a list of disease conditions in a Shared Disease Grouping (as defined herein) and list of participating LHJs in a Shared Jurisdiction Grouping (as defined herein). Designated Users (as defined herein) are granted a read-only user account with permissions to access the Shared Disease Grouping, and Shared Jurisdiction Grouping, which allows these users access to these data from their own and other participating jurisdictions.

II. Definitions: For purposes of this Exhibit, the following definitions shall apply in addition to those set forth in the Agreement:

A. CalREDIE Data: "CalREDIE Data" means data in the state-wide reportable disease database supported and maintained by CDPH including demographic, epidemiologic (including clinical information, risk factor information, and laboratory test result information), and administrative information on reportable diseases collected for the purposes of case investigation, disease prevention, and surveillance.

1. CalREDIE Data specifically includes information contained in or derived from the following:

a. Confidential Morbidity Report (CMR) required by Title 17 of the California Code of Regulations (CCR) sections 2500, 2593, 2641.5-2643.20, and 2800-2812 Reportable Diseases and Conditions.

b. Laboratory Test and Result information required by Title 17 of the CCR sections 2505 and 2641.5 - 2643.20.

c. Communicable Disease Control Report Forms.(obtained from healthcare providers, laboratories, and local health departments pursuant to state and federal law including but not limited to Title 17 CCR sections 2500 et seq.)

B. Designated Users: "Designated Users" means individuals from Recipient's jurisdiction granted a read-only user account with permissions to access the Shared Disease Grouping and Shared Jurisdiction Grouping. Designated Users are only permitted read-only access to both Recipient's data and the data from other participating jurisdictions. Each Recipient may designate up to three (3) individuals as Designated Users.

C. Shared Disease Grouping: "Shared Disease Grouping" means the list of corresponding disease conditions in CalREDIE. Any diseases included in the Shared Disease Grouping will continue to be included regardless of future name changes. Additional diseases may be added to the Shared Disease Grouping at the request of the California Conference of Local Health Officers.

1. For example, corresponding conditions in the viral hepatitis and syphilis shared grouping are:

a. Hepatitis B, Acute
b. Hepatitis B, Chronic
c. Hepatitis C, Acute
d. Hepatitis C, Chronic
e. Hepatitis D (Delta)
f. Hepatitis E, Acute
g. Syphilis (Congenital)
h. Syphilis (Early Latent)
i. Syphilis (Late with Clinical Manifestations)
j. Syphilis (Latent, Unknown Duration)
k. Syphilis (Primary)
l. Syphilis (Secondary)
m. Syphilis State Unknown/Reactor
n. Syphilis Initial Report

D. Shared Jurisdictional Grouping: "Shared Jurisdictional Grouping" means the list of LHJs participating in cross jurisdictional sharing. The Local Health Officer (LHO) for Recipient may opt-in to participate in cross-jurisdictional data sharing, which means the Recipient agrees to share its data for the Shared Disease Grouping in a read-only fashion with other LHJs.

III. Legal Authority for Collection, Use and Disclosure of CalREDIE Data: The legal authority for CDPH and Recipient to collect, use and disclose CalREDIE Data include the following:

1. California Civil Code section 1798.24(e);
2. California Health and Safety Code section 120175;
3. Title 17 California Code of Regulations section 2502.

IV. Permitted Uses and Disclosures: Recipient and its Designated Users shall safeguard the CalREDIE Data to which they have access to from unauthorized use and disclosure. Recipient and its Designated Users shall not use or disclose any CalREDIE Data, Shared Disease Grouping data, or Shared Jurisdictional Grouping data for any purpose other than carrying out the Recipient's obligations under the statutes and regulations set forth in this Exhibit, or as otherwise allowed or required by state or federal law.

V. Restricted Disclosures and Uses: Recipient shall limit the access it provides to its Designated Users to the minimum necessary. Additionally, should the Recipient determine a Designated User's duties require access to any CalREDIE Data or Shared Disease Grouping data related to HIV, Recipient is responsible for instructing the Designated User as to their responsibilities under the law. Recipient will have the Designated User sign the HIV Confidentiality Acknowledgement and then maintain a copy of the Acknowledgement in their records, as well as provide a copy of the Acknowledgement to CDPH.

VI. Disclaimer: CDPH makes no warranty or representation that data provided to Recipient pursuant to its compliance with this Exhibit will be adequate or satisfactory for Recipient's own purposes or that any information in Recipient's possession or control, or transmitted or received by Recipient, is or will be secure from unauthorized use or disclosure. Recipient is solely responsible for all decisions made by Recipient regarding the safeguarding of CalREDIE Data, Shared Disease Grouping data, or Shared Jurisdictional Grouping data.

VII. Contact Information: To direct communications to the other party regarding this Exhibit, CDPH or Recipient shall use the contact information below. The Parties reserve the right to make changes to the

contact information below by verbal or written notice. Changes do not require an amendment to this Exhibit.

CDPH Program Manager	CDPH Privacy Officer	CDPH Chief Information Security Officer and CDPH IT Service Desk
Abigail Kroch, PhD MPH Branch Chief, Public Health Reporting Information Exchange (PRIME) Division of Communicable Disease Control California Department of Public Health Phone: 916.720.8268 Abigail.Kroch@cdph.ca.gov	**Privacy Officer** Privacy Office c/o Office of Legal Services California Dept. of Public Health P.O. Box 997377, MS 0506 Sacramento, CA 95899-7377 Email: privacy@cdph.ca.gov Telephone: (877) 421-9634	**Chief Information Security Officer** Information Security Office California Dept. of Public Health P.O. Box 997413, MS 6300 Sacramento, CA 95899-7413 Email: cdph.infosecurityoffice@cdph.ca.gov Telephone: (800) 500-0016
Recipient Program Manager	**Recipient Privacy Officer**	**Recipient Information Security Officer**

Exhibit G - CalCONNECT Cross-Jurisdictional Data Sharing Policy/Procedure

Purpose

This **CalCONNECT Cross-Jurisdictional Data Sharing Policy and Procedure** provides guidance to state and local public health staff regarding how CalCONNECT data can be shared across jurisdictions, in an authorized and secure manner.

Background

The implementation of CalCONNECT as a contact tracing tool to support disease surveillance efforts in California has introduced changes and, in general, increased efficiency in how state and local health jurisdiction staff access and share surveillance data. However, to date, the ability to share contact tracing data across jurisdictions was restricted, limiting public health activities.

Summary

- CalCONNECT shall contain a "shared" disease list of conditions.
- Participating Local Health Jurisdictions (LHJs) shall be included in a "shared" jurisdiction grouping.
- Designated individuals from participating LHJs shall be granted a read-only user account with permissions to access the "shared" disease list of conditions, and the "shared" jurisdiction conditions, to allow these users read-only access to the shared disease data from their own and the other participating jurisdictions.
- Participating LHJs also acknowledge that disease specific CalCONNECT Data will also be coming from other CDPH databases like CAIR and CalREDIE and across all participating counties once the LHJ agrees to participate in a "shared" jurisdiction grouping. However, in all instances, CDPH will only be sharing CalCONNECT Data from participating LHJs that are both "necessary and relevant" for purposes of contact tracing, case investigation and for examining the causes of the Contagious Infectious, or Communicable or Reportable Diseases and Conditions, to ascertain the nature of the disease or condition and to prevents its spread that directly or indirectly relates to an individual.

Shared Disease Grouping

- A list of disease conditions in CalCONNECT shall be included in a "shared" disease list of conditions for participating LHJs.
    - To pilot this effort, CalCONNECT will start with covid-19, tuberculosis, mpox, and STD/HIV. The corresponding list of disease conditions in CalCONNECT are:
        - Covid-19 case
        - Covid-19 contact
        - Tuberculosis case
        - Tuberculosis contact
        - STD/HIV case [1]
        - STD/HIV contact [1]
        - Mpox case
        - Mpox contact
    - If these conditions undergo name changes in the CalCONNECT application, they will

[1] For information related to either STD/HIV, all individuals must sign the confidentiality requirement form specific to HIV/AIDS prior to accessing the data.

continue to be included in the shared disease list of conditions.
    - Additional diseases may be added to this disease list of conditions, at the request of the California Conference of Local Health Officers (CCLHO) and upon review and approval of CDPH.

Shared Jurisdiction Grouping

- Participating Local Health Jurisdictions (LHJs) shall be included in a "shared" jurisdiction grouping in CalCONNECT.
    - Local Health Officers (LHOs) may "opt-in" to participate in cross-jurisdictional data sharing, which means that they agree to share their LHJ's data for the "shared" disease conditions with other participating LHJs.
    - To opt-in to cross-jurisdictional data sharing, the Local Health Officer must complete, sign, and submit to the CalCONNECT Help Desk, the attached form, CalCONNECT Cross- Jurisdictional Data Sharing Authorization Form, authorizing to share, in a read-only fashion, with other participating LHJs their data for the conditions in the shared disease grouping.

Designated Users

- Designated individuals from participating LHJs shall be granted a read-only user account with permissions to access the "shared" disease grouping and the "shared" jurisdiction grouping. These read-only accounts will allow designated users read-only access to their data and the data from the other participating jurisdictions.

Health Officer Emergency Authorities

LHOs have general broad authority to take all measures necessary to prevent the spread of disease:

H&SC section 120175. The Local Health Officer, having reason to believe that any case of a communicable disease exists within his/her jurisdiction, has the authority to take measures necessary to prevent the spread of the disease.

17 CCR section 2502, a regulation which discusses LHO required gathering of individual case reports and weekly morbidity reports for certain reportable diseases and submission of these reports to CDPH, provides for instances when an LHO may share this infectious disease reportable data with another LHO, including, to determine the existence of a disease, its cause, or the measures necessary to stop its spread or, for purposes of his/her investigation, as may be necessary to prevent the spread or occurrence of additional cases:

(f) Confidentiality. Information reported pursuant to this section is acquired in confidence and shall not be disclosed by the local health officer except as authorized by these regulations, as required by state or federal law, or with the written consent of the individual to whom the information pertains or to the legal representative of that individual.

> (1) A health officer shall disclose any information, including personal information, contained in an individual case report to state, federal or local public health officials in order to determine the existence of a disease, its likely cause or the measures necessary to stop its spread.
>
> (2) A health officer may for purposes of his or her investigation disclose any information contained in an individual case report, including personal information, as may be necessary to prevent the spread of disease or occurrence of additional cases.

1. Opt-in – To be completed by the Health Officer

I, Sharon Wang, DO, MSHPE, FIDSA, authorize San Bernardino County Department of Public Health data for all Contagious, Infectious, Communicable or Reportable Diseases and Conditions (as defined in the Data Use and Disclosure Agreement of the CalCONNECT System)(hereinafter "Diseases and Conditions") in CalCONNECT to be shared with jurisdictions participating in CalCONNECT cross-jurisdictional data sharing (hereinafter " Shared Jurisdictions") for the purpose of examining the causes of the Diseases and Conditions, and to ascertain the nature of the Diseases or Conditions to prevent its spread. I also acknowledge that an individual's patient history as it may relate to all Diseases and Conditions may be shared as necessary, with all other jurisdictions participating which may include lab test results, contacts, prior history and exposure etc. I further attest, that by executing this document, I understand that all information related to any individual that my county collects in the CalCONNECT system, which may include symptoms and conditions, will be visible to the other Shared Jurisdictions.

Name (Print): Sharon Wang, DO,MSHPE, FIDSA Title: Health Officer E-mail: Sharon.Wang@dph.sbcounty.gov

2. Health Officer Approval

Sharon Wang, DO, MSHPE, FIDSA		
Name (Print)	Name (Signature)	Date

3. Delegate authorization

The Health Officer (above) appoints the following Authorized Representative to add CalCONNECT System User(s) for Shared Jurisdiction User(s).