STATE OF CALIFORNIA

STANDARD AGREEMENT

STD 213 (Rev 02/20)

AGREEMENT NUMBER	REGISTRATION NUMBER
20-10777	

STATE CONTROLLER'S OFFICE IDENTIFIER
4265-2010777

1. This Agreement is entered into between the State Agency and the Contractor named below:

STATE AGENCY'S NAME
California Department of Public Health, hereinafter referred to as "State"

CONTRACTOR'S NAME
UC San Diego Health, hereinafter referred to as "University"

2. The term of this Agreement is: 11/18/2020 through 11/30/2021

3. The maximum amount of this Agreement is: **$** 2,000,000.00

4. The Parties agree to comply with the terms and conditions of the following Exhibits, which by this reference are made a part of the Agreement.

Exhibit A – **A7**: A–Scope of Work; A1a & b –Scope of Work / Proposal; A2–Key Personnel; A3–Authorized Representatives; A4–Use of Intellectual Property & Data; A5–Resumes/Biosketch; A6–Current & Pending Support; A7-Third Party Confidential Information	14 page(s)
Exhibit B – B–Budget; B1–Budget Justification; B2– Subawardee Budgets (if applicable); B3–Invoice Elements	5 page(s)
Exhibit C* – University Terms and Conditions	UTC-220

Check mark additional Exhibits below, and attach applicable Exhibits or provide internet link:

☒ **Exhibit D** – Additional Requirements Associated with Funding Sources	4	page(s)
☒ **Exhibit E** – Special Conditions for Security of Confidential Information	3	page(s)
☒ **Exhibit F** – Information Privacy and Security Requirements	12	page(s)
☐ **Exhibit G** – Negotiated Alternate UTC Terms		page(s)

Items shown with an Asterisk (*) are hereby incorporated by reference and made part of this agreement as if attached hereto. You can find these documents on the University of California, Office of the President and the California Department of General Services websites.

IN WITNESS WHEREOF, this Agreement has been executed by the Parties hereto.

CONTRACTOR

CONTRACTOR'S NAME *(if other than an individual, state whether a corporation, partnership, etc.)*
UC San Diego Health

BY *(Authorized Signature)*: DocuSigned by: [redacted]

DATE SIGNED *(Do not type)*: 12/4/2020

PRINTED NAME AND TITLE OF PERSON SIGNING
Patty Maysent, CEO UC San Diego Health

ADDRESS
9560 Towne Centre Drive, San Diego, CA 92121

STATE OF CALIFORNIA

AGENCY NAME
California Department of Public Health

BY *(Authorized Signature)*:

DATE SIGNED *(Do not type)*:

PRINTED NAME AND TITLE OF PERSON SIGNING
Tim Bow, Procurement Officer

ADDRESS
1615 Capitol Ave, Sacramento, CA 95814

California Department of General Services Use Only

☒ Exempt per: PCC 1102
Executive Order N-25-20-COVID19

Exhibit A – Scope of Work

Project Summary & Scope of Work

☒ Contract ☐ Grant

Does this project include Research (as defined in the UTC)? ☐ Yes ☒ No

PI Name: Nicole May

Project Title: Click or tap here to enter text.

Project Summary/Abstract

Briefly describe the long-term objectives for achieving the stated goals of the project.

Contractor agrees to provide to the California Department of Public Health (CDPH) the services described herein.

UC San Diego Health (UCSDH) will provide comprehensive project implementation support for the roll-out of the Google/Apple Covid-19 Exposure Notification Express System (ENX) in California, as well as post-implementation operational support for the program.

If Third-Party Confidential Information is to be provided by the State:

☐ Performance of the Scope of Work is anticipated to involve use of third-party Confidential Information and is subject to the terms of this Agreement; ***OR***

☐ A separate CNDA between the University and third-party is required by the third-party and is incorporated in this Agreement as Exhibit A7, Third Party Confidential Information.

Scope of Work

Describe the goals and specific objectives of the proposed project and summarize the expected outcomes. If applicable, describe the overall strategy, methodology, and analyses to be used. Include how the data will be collected, analyzed, and interpreted as well as any resource sharing plans as appropriate. Discuss potential problems, alternative strategies, and benchmarks for success anticipated to achieve the goals and objectives.

Click or tap here to enter text.

*See Attached Exhibit A1a and b - Services & Deliverables

Exhibit A, Attachment 1a

1. Services to be Performed

A. Program & Project Management. UCSDH will supply 4 full-time project management resources. They will provide the following: general organization for the program and lead project work; manage project activities, timelines, and risks; maintain and archive project documentation; organize meetings; coordinate communication between stakeholder groups; prepare the project for close-out and hand-off; and perform other project management work as necessary.

B. Call Center Management. UCSDH will establish and manage a call center to provide the following: code verification and distribution for COVID-19 positive ENX users; technical support and general information for ENX users and Local Health Jurisdictions (LHJs); and public health guidance for ENX users. UCSDH will expand its current call center operations to accommodate call volumes generated by ENX. It is anticipated that this call center will be the primary source for ENX users to retrieve key codes and get public health guidance at the outset of the ENX roll-out. When these process are automated after implementation, the call center will become the secondary source for this information.

C. Code Distribution Automation. UCSDH will provide an integration engineer to coordinate, design, and execute technical activities associated with automating the code distribution process. This engineer may work in concert with CDPH and/or CDT engineers assigned to the same task.

D. CA Covid Notify Website. UCSDH will develop and maintain the landing and exposure notification web pages for ENX. UCSDH will supply a team of web developers, technology human factors engineers, health marketing experts, and population health researchers to create and update evidence-based content to encourage adoption of ENX.

E. Marketing and Communications. UCSDH will provide marketing and communications assets developed during the pilot program for ENX, along with consulting services to improve user adoption and experience based on UCSDH's previous ENX pilots. UCSDH will coordinate marketing and communications efforts for the ENX roll-out.

F. Analytics. UCSDH will ensure data regarding the performance of ENX are captured and made ready for presentation.

G. Transition to Operations. UCSDH will ensure that all elements of the exposure notification program under UCSDH's management that are required for the successful operation of the program are successfully transitioned to CDPH's management at the end of this contract.

2. CDPH Responsibilities

A. CDPH will provide UCSDH the following:

1. Access to ENX, as configured for the State of California.

2. Updates to the ENX Configuration File as determined necessary by CDPH, including maintenance and updates of the California Risk Model for exposure notification.

3. Administrative access to the ENX Verification Server.

4. A Twilio Account used to send Verification Codes via SMS text.

5. Access to records needed to verify a positive COVID-19 diagnosis, so that UCSDH Call Center can issue verification codes on behalf of the State of California and Local Health Jurisdictions.

6. A primary point of contact at CDPH who will be responsible to facilitate decision making and issue resolution related to public health program decisions.

7. A primary point of contact at CDT who will be responsible for overall coordination of the ENX program, and access to CDT technical resources as needed.

8. Primary communication with Local Health Jurisdictions, and assistance to UCSDH in coordination with LHJs as may be needed to plan, schedule, train or otherwise coordinate local implementation with the LHJs.

9. Updates to CalCONNECT scripts for Case Investigators and integration with CalCONNECT for verification code distribution, should that integration be desired by the State.

10. Technical resources to work with UCSDH engineer on integration of the Verification Server with other systems such as CCRS, labs, medical systems, or other points as may be desired by the State.

11. Access and resources for website enablement.

12. Any paid marketing that the State desires will be the sole responsibility of the State. UCSDH will provide marketing assets that may be used by the State in marketing campaigns.

November 17, 2020

UC San Diego Health
Information Services
9560 Towne Centre Drive
San Diego, CA 92121

Christopher A. Longhurst, MD, MS
CIO and Associate CMO
Program Sponsor

Nicole May, MHSA
Director, PMO
Program Contact
nmay@health.ucsd.edu
(281) 382-3421

Proposal for Implementation Services

Statewide Roll-out of COVID 19 Exposure Notification System

Program Description

UC San Diego Health (UCSDH) proposes to provide comprehensive project implementation support for the roll-out of the Google/Apple Covid-19 Exposure Notification Express System (ENX) in California, as well as post-implementation operational support for the program.

ENX is privacy-preserving technology developed by Google and Apple that has the capability to quickly notify users who may have been exposed to COVID-19 and may reduce the spread of this disease in our communities. The California Department of Public Health (CDPH) and the California Department of Technology (CDT) previously partnered with UCSDH to pilot ENX on its campus and at 6 other University of California campuses prior to this proposed state-wide roll-out.

UCSDH's proposal includes the following:

1. Program & Project Management. UCSDH will supply 4 full-time project management resources. They will provide the following: general organization for the program and lead project work; manage project activities, timelines, and risks; maintain and archive project documentation; organize meetings; coordinate communication between stakeholder groups; prepare the project for close-out and hand-off; and perform other project management work as necessary.

2. Call Center Management. UCSDH will establish and manage a call center to provide the following: code verification and distribution for COVID-19 positive ENX users; technical support and general information for ENX users and Local Health Jurisdictions (LHJs); and public health guidance for ENX users. UCSDH will expand its current call center operations to accommodate call volumes generated by ENX. It is anticipated that this call center will be the primary source for ENX users to retrieve key codes and get public health guidance at the outset of the ENX roll-out. When these process are automated after implementation, the call center will become the secondary source for this information.

3. Code Distribution Automation. UCSDH will provide an integration engineer to coordinate, design, and execute technical activities associated with automating the code distribution process. This engineer may work in concert with CDPH and/or CDT engineers assigned to the same task.

4. CA Covid Notify Website. UCSDH will develop and maintain the landing and exposure notification web pages for ENX. UCSDH will supply a team of web developers, technology human factors engineers, health marketing experts, and population health researchers to create and update evidence-based content to encourage adoption of ENX.

5. Marketing and Communications. UCSDH will provide marketing and communications assets developed during the pilot program for ENX, along with consulting services to improve user adoption and experience based on UCSDH's previous ENX pilots. UCSDH will coordinate marketing and communications efforts for the ENX roll-out.
6. Analytics. UCSDH will ensure data regarding the performance of ENX are captured and made ready for presentation.
7. Transition to Operations. UCSDH will ensure that all elements of the exposure notification program under UCSDH's management that are required for the successful operation of the program are successfully transitioned to CDPH's management at the end of this contract.

The State of California will provide UCSDH:

13. Access to ENX, as configured for the State of California.
14. Updates to the ENX Configuration File as determined necessary by CDPH, including maintenance and updates of the California Risk Model for exposure notification.
15. Administrative access to the ENX Verification Server.
16. A Twilio Account used to send Verification Codes via SMS text.
17. Access to records needed to verify a positive COVID-19 diagnosis, so that UCSDH Call Center can issue verification codes on behalf of the State of California and Local Health Jurisdictions.
18. A primary point of contact at CDPH who will be responsible to facilitate decision making and issue resolution related to public health program decisions
19. A primary point of contact at CDT who will be responsible for overall coordination of the ENX program, and access to CDT technical resources as needed.
20. Primary communication with Local Health Jurisdictions, and assistance to UCSDH in coordination with LHJs as may be needed to plan, schedule, train or otherwise coordinate local implementation with the LHJs.
21. Updates to CalCONNECT scripts for Case Investigators and integration with CalCONNECT for verification code distribution, should that integration be desired by the State.
22. Technical resources to work with UCSDH engineer on integration of the Verification Server with other systems such as CCRS, labs, medical systems, or other points as may be desired by the State.
23. Access and resources for website enablement.
24. Any paid marketing that the State desires will be the sole responsibility of the State. UCSDH will provide marketing assets that may be used by the State in marketing campaigns.

Budget

The below cost is based on a call volume of up to 20,000 per week.

Call Center Support				
Start	**End**	**Expense Type**	**Monthly Rate**	**Total**
1-Dec-20	31-May-21	Call Center Manager (1.0)	$ 15,833	$ 95,000
1-Dec-20	31-May-21	Health Line Call Center Staff Operations	$ 50,800	$ 304,800
7-Dec-20	29-Jan-21	Tech and Code Line Call Center Operations	$ 581,175	$ 1,162,350
		Total Cost		$ 1,562,150

Project Management Support				
Start	**End**	**Expense Type**	**Monthly Rate**	**Total**
1-Dec-20	31-May-21	Program Manager (1.0)	$ 20,833	$ 125,000
1-Dec-20	31-May-21	Project Manager (1.0)	$ 12,500	$ 75,000
1-Dec-20	31-Jan-21	Project Manager (1.0)	$ 12,500	$ 25,000
1-Dec-20	31-Jan-21	Project Manager (1.0)	$ 12,500	$ 25,000
		Total Cost		$ 250,000

Web Design/Support and Marketing Consulting				
Start	**End**	**Expense Type**	**Monthly Rate**	**Total**
1-Dec-20	31-Jan-21	Design Firm	$ 25,000	$ 50,000
1-Dec-20	31-May-21	Developer (0.25)	$ 3,958	$ 23,750
1-Dec-20	31-Jan-21	Translation Services	$ 5,000	$ 10,000
		Total Cost		$ 83,750

Integration Support				
Start	**End**	**Expense Type**	**Monthly Rate**	**Total**
1-Dec-20	31-Jan-21	Engineer (1.0)	$ 15,833	$ 31,667
		Total Cost		$ 31,667

Allowance for Unanticipated Costs				
1-Dec-20	31-May-21			**Total**
		Total Cost		$ 20,000

Grand Total	**$ 1,947,567**

Exhibit A1 - Deliverables

SCHEDULE OF DELIVERABLES

List all items that will be delivered to the State under the proposed Scope of Work. Include all reports, including draft reports for State review, and any other Deliverables, if requested by the State and agreed to by the Parties.

If use of any Deliverable is restricted or is anticipated to contain preexisting Intellectual Property with any restricted use, it will be clearly identified in Exhibit A4, Use of Preexisting Intellectual Property & Data.

Unless otherwise directed by the State, the University Principal Investigator shall submit all Deliverables to the State Contract Project Manager, identified in Exhibit A3, Authorized Representatives.

Deliverable	Description	Due Date
The following Deliverables are subject to Section 19. Copyrights, paragraph B of Exhibit C		

Exhibit A2 – Key Personnel

KEY PERSONNEL

List Key Personnel as defined in the Agreement starting with the PI, by last name, first name followed by Co-PIs. Then list all other Key Personnel in alphabetical order by last name. For each individual listed include his/her name, institutional affiliation, and role on the proposed project. Use additional consecutively numbered pages as necessary.

Last Name, First Name	Institutional Affiliation	Role on Project
PI:		
Last name, First name	*Institutional affiliation*	*Role on the project*
Co-PI(s) – if applicable:		
Last name, First name	*Institutional affiliation*	*Role on the project*
Last name, First name	*Institutional affiliation*	*Role on the project*
Other Key Personnel (if applicable):		
Last name, First name	*Institutional affiliation*	*Role on the project*
Last name, First name	*Institutional affiliation*	*Role on the project*

Exhibit A3 – Authorized Representatives

AUTHORIZED REPRESENTATIVES AND NOTICES

The following individuals are the authorized representatives for the State and the University under this Agreement. Any official Notices issued under the terms of this Agreement shall be addressed to the Authorized Official identified below, unless otherwise identified in the Agreement.

State Agency Contacts	**University Contacts**
Agency Name: CDPH	University Name: UC San Diego Health
Contract Project Manager (Technical) Name: Carolyn Nordstrom Address: 1325 J Street, 16th Floor Sacramento, CA 95814 Telephone: 916-215-9837 Fax: N/A Email: Carolyn.nordstrom@cdph.ca.gov	***Principal Investigator*** Name: Nicole May Address: 9560 Towne Centre Drive San Diego, CA 92121 Telephone: 281-382-3421 Fax: N/A Email: nmay@health.ucsd.edu Designees to certify invoices under Section 14 of Exhibit C on behalf of PI: 1. N/A
Authorized Official (contract officer) Name: Same as above Address: Telephone: Fax: Email: ***Send notices to (if different):*** Name: Same as Above Address: Telephone: Email:	***Authorized Official*** Name: Same as above Address: Telephone: Fax: Email: ***Send notices to (if different):*** Name: Same as above Address: Telephone: Email:
Administrative Contact Name: Same as above	***Administrative Contact*** Name: Same as above

Address: Telephone: Fax: Email:	Address: Telephone: Fax: Email:
Financial Contact/Accounting Name: Phebe Lapinig Address: California Department of Public Health Emergency Preparedness Office MS 7002 1615 Capitol Ave, 73.373 Sacramento, CA 95814 Telephone: 916-210-1570 Fax: Email: phebe.lapinig@cdph.ca.gov	***Authorized Financial Contact/Invoicing/Remittance*** Name: Same as above Address: Telephone: Fax: Email: Designees for invoice certification in accordance with Section 14 of Exhibit C on behalf of the Financial Contact: 1.

Exhibit A4 – Use of Intellectual Property & Data

USE OF INTELLECTUAL PROPERTY & DATA

If either Party will be using any third-party or pre-existing intellectual property (including, but not limited to copyrighted works, known patents, trademarks, service marks and trade secrets) "IP" and/or Data with restrictions on use, then list all such IP/Data and the nature of the restriction below. If no third-party or pre-existing IP/Data will be used, check "none" in this section.

A. State: Preexisting IP/Data to be provided to the University from the State or a third party for use in the performance in the Scope of Work.

☒ None or ☐ List:

Owner (Name of State Agency or 3rd Party)	Description	Nature of restriction:

B. University: Restrictions in Preexisting IP/Data included in Deliverables identified in Exhibit A1, Deliverables.

☒ None or ☐ List:

Owner (Name of University or 3rd Party)	Description	Nature of restriction:

C. Anticipated restrictions on use of Project Data.

If the University PI anticipates that any of the Project Data generated during the performance of the Scope of Work will have a restriction on use (such as subject identifying information in a data set) then list all such anticipated restrictions below. If there are no restrictions anticipated in the Project Data, then check "None" in this section.

☒ None or ☐ List:

Owner (University or 3rd Party)	Description	Nature of Restriction:

Exhibit A5 - RÉSUMÉ/BIOSKETCH

RÉSUMÉ/BIOSKETCH

Attach 2-3 page Resume/Biosketch for the PI and other Key Personnel listed in Exhibit A2, Key Personnel.

Exhibit A6 – Current & Pending Support

CURRENT & PENDING SUPPORT

University will provide current & pending support information for Key Personnel identified in Exhibit A2 at time of proposal and upon request from State agency. The "Proposed Project" is this application that is submitted to the State. Add pages as needed.

PI: Nicole May

Status (currently active or pending approval)	Award # (if available)	Source (name of the sponsor)	Project Title	Start Date	End Date
Proposed Project					
CURRENT					
CURRENT					
PENDING					

NAME OF INDIVIDUAL

Status	Award #	Source	Project Title	Start Date	End Date
Proposed Project					
CURRENT					
CURRENT					
PENDING					

NAME OF INDIVIDUAL

Status	Award #	Source	Project Title	Start Date	End Date
Proposed Project					
CURRENT					
CURRENT					
PENDING					

NAME OF INDIVIDUAL

Status	Award #	Source	Project Title	Start Date	End Date
Proposed Project					
CURRENT					
CURRENT					
PENDING					

NAME OF INDIVIDUAL

Status	Award #	Source	Project Title	Start Date	End Date
Proposed Project					
CURRENT					
CURRENT					
PENDING					

Exhibit A7

Third Party Confidential Information

Confidential Nondisclosure Agreement

(Identified in Exhibit A, Scope of Work – will be incorporated, if applicable)

If the Scope of Work requires the provision of third party confidential information to either the State or the Universities, then any requirement of the third party in the use and disposition of the confidential information will be listed below. The third party may require a separate Confidential Nondisclosure Agreement (CNDA) as a requirement to use the confidential information. Any CNDA will be identified in this Exhibit A7.

Exhibit B - Budget

Budget for Project Period

Principal Investigator (Last, First): Nicole May

Exhibit B

COMPOSITE BUDGET FOR ENTIRE PROPOSED PROJECT PERIOD
11/18/2020 to 11/30/2021

	From: To:	
BUDGET CATEGORY		**TOTAL**
PERSONNEL: *Salary and fringe benefits.*		$2,000,000.00
TRAVEL		$0
MATERIALS & SUPPLIES		$0
EQUIPMENT		$0
CONSULTANT		$0
SUBRECIPIENT		$0
OTHER DIRECT COSTS (ODC)	***Subject to IDC Calc***	
TOTAL DIRECT COSTS		**$0**
Indirect (F&A) Costs	**F&A Base**	
Rate	***MTDC ****	*$0*
		$0
TOTAL COSTS PER YEAR		
TOTAL COSTS FOR PROPOSED PROJECT PERIOD		**$2,000,000.00**

* MTDC = Modified Total Direct Cost

See Exhibit A, Attachment 1b for cost details

Exhibit B1

Budget Justification

The Budget Justification will include the following items in this format.

Personnel

Name. *Starting with the Principal Investigator list the names of all known personnel who will be involved on the project for each year of the proposed project period. Include all collaborating investigators, individuals in training, technical and support staff or include as "to be determined" (TBD).*

Role on Project. *For all personnel by name, position, function, and a percentage level of effort (as appropriate), including "to-be-determined" positions.*

Fringe Benefits.
In accordance with University policy, explain the costs included in the budgeted fringe benefit percentages used, which could include tuition/fee remission for qualifying personnel to the extent that such costs are provided for by University policy, to estimate the fringe benefit expenses on Exhibit B.

Travel

Itemize all travel requests separately by trip and justify in Exhibit B1, in accordance with University travel guidelines. Provide the purpose, destination, travelers (name or position/role), and duration of each trip. Include detail on airfare, lodging and mileage expenses, if applicable. Should the application include a request for travel outside of the state of California, justify the need for those out-of-state trips separately and completely.

Materials and Supplies

Itemize materials supplies in separate categories. Include a complete justification of the project's need for these items. Theft sensitive equipment (under $5,000) must be justified and tracked separately in accordance with State Contracting Manual Section 7.29.

Equipment

List each item of equipment (greater than or equal to $5,000 with a useful life of more than one year) with amount requested separately and justify each.

Consultant Costs

Consultants are individuals/organizations who provide expert advisory or other services for brief or limited periods and do not provide a percentage of effort to the project or program. Consultants are not involved in the scientific or technical direction of the project as a whole. Provide the names and organizational affiliations of all consultants. Describe the services to be performed, and include the number of days of anticipated consultation, the expected rate of compensation, travel, per diem, and other related costs.

Subawardee (Consortium/Subrecipient) Costs

Each participating consortium organization must submit a separate detailed budget for every year in the project period in Exhibit B2 Subcontracts. Include a complete justification for the need for any subawardee listed in the application.

Other Direct Costs

Itemize any other expenses by category and cost. Specifically justify costs that may typically be treated as indirect costs. For example, if insurance, telecommunication, or IT costs are charged as a direct expense, explain reason and methodology.

Rent

If the Scope of Work will be performed in an off-campus facility rented from a third party for a specific project or projects, then rent may be charged as a direct expense to the award.

Indirect (F&A) Costs

Indirect costs are calculated in accordance with the budgeted indirect cost rate in Exhibit B.

Exhibit B2 – Subawardee Budgets

Budget Pertaining to Subawardee(s) (when applicable)

Subawardee Name:

Principal Investigator (Last, First):

Exhibit B2

COMPOSITE SUBAWARDEE BUDGET FOR ENTIRE PROPOSED PROJECT PERIOD
07/01/2016 to 06/30/2019

From: / To:		7/1/2016 6/30/2017	7/1/2017 6/30/2018	7/1/2018 6/30/2019	
BUDGET CATEGORY		**Year 1**	**Year 2**	**Year 3**	**TOTAL**
PERSONNEL: *Salary and fringe benefits.*		$0	$0	$0	$0
TRAVEL		$0	$0	$0	$0
MATERIALS & SUPPLIES		$0	$0	$0	$0
EQUIPMENT		$0	$0	$0	$0
CONSULTANT		$0	$0	$0	$0
SUBRECIPIENT		$0	$0	$0	$0
OTHER DIRECT COSTS (ODC)	***Subject to IDC Calc***				
ODC #1	***Y***	$0	$0	$0	$0
ODC #2	***Y***	$0	$0	$0	$0
ODC #3	***Y***	$0	$0	$0	$0
ODC #4	***Y***	$0	$0	$0	$0
ODC #5	***Y***	$0	$0	$0	$0
ODC #6	***Y***	$0	$0	$0	$0
TOTAL DIRECT COSTS		**$0**	**$0**	**$0**	**$0**
Indirect (F&A) Costs	**F&A Base**				
Rate	***MTDC ****	*$0*	*$0*	*$0*	*$0*
		$0	**$0**	**$0**	**$0**
TOTAL COSTS PER YEAR		**$0**	**$0**	**$0**	
TOTAL COSTS FOR PROPOSED PROJECT PERIOD					**$0**

* MTDC = Modified Total Direct Cost

JUSTIFICATION. *See Exhibit B1 - Follow the budget justification instructions.*

Annual Budget Flexibility (lesser of % or Amount)

Prior approval required for budget changes between approved budget categories above the thresholds identified.

% **10.00%**

or

Amount *$10,000*

Exhibit B3 – Invoice Elements

Invoice and Detailed Transaction Ledger Elements

In accordance with Section 14 of Exhibit C – Payment and Invoicing, the invoice, summary report and/or transaction/payroll ledger shall be certified by the University's Financial Contact and the PI (or their respective designees).

Invoicing frequency

☐ Quarterly ☐ Monthly

Invoicing signature format

☐ Ink ☐ Facsimile/Electronic Approval

Summary Invoice – includes either on the invoice or in a separate summary document – by approved budget category (Exhibit B) – expenditures for the invoice period, approved budget, cumulative expenditures and budget balance available[1]

- Personnel
- Equipment
- Travel
- Subawardee – Consultants
- Subawardee – Subcontract/Subrecipients
- Materials & Supplies
- Other Direct Costs
    - TOTAL DIRECT COSTS (if available from system)
- Indirect Costs
    - TOTAL

Detailed transaction ledger and/or payroll ledger for the invoice period [2]

- University Fund OR Agency Award # (to connect to invoice summary)
- Invoice/Report Period (matching invoice summary)
- GL Account/Object Code
- Doc Type (or subledger reference)
- Transaction Reference#
- Transaction Description, Vendor and/or Employee Name
- Transaction Posting Date
- Time Worked
- Transaction Amount

[1] If this information is not on the invoice or summary attachment, it may be included in a detailed transaction ledger.

[2] For salaries and wages, these elements are anticipated to be included in the detailed transaction ledger. If all elements are not contained in the transaction ledger, then a separate payroll ledger may be provided with the required elements.

Exhibit C – University Terms and Conditions

CMA (AB20) State/University Model Agreement Terms & Conditions UTC-220

Exhibit D- Additional Requirements Associated with Funding Sources

(if applicable)

If the Agreement is subject to any additional requirements imposed on the funding State agency by applicable law (including, but not limited to, bond, proposition and federal funding), then these additional requirements will be set forth in Exhibit D. If the University is a subrecipient, as defined in 2 CFR 200 (Uniform Guidance on Administrative Requirements, Audit Requirements and Cost Principles for Federal Financial Assistance), and the external funding entity is the federal government, the below table must be completed by the State agency. (Please see sections 10.A and 10.B of the Exhibit C.)

Federal Emergency Management Agency (FEMA) Requirements

1.1 Changes

Any cost of a change, modification, change order, or constructive change to the Agreement must be allowable and allocable within the scope of this Agreement, and reasonable for the completion of project scope. Changes can be made by either Party to alter the method, price, or schedule of the work without breaching the Agreement if both Parties approve in writing.

1.2 Compliance with Federal Law, Regulations, and Executive Orders

This is an acknowledgement that FEMA financial assistance will be used to fund all or a portion of the contract only. The Contractor will comply with all federal law, regulations, executive orders, FEMA policies, procedures, and directives.

1.3 No Obligation by Federal Government

The Federal Government is not a party to this contract and is not subject to any obligations or liabilities to the non-Federal entity, Contractor, or any other party pertaining to any matter resulting from the contract.

1.4 Program Fraud and False or Fraudulent Statements or Related Acts

The Contractor acknowledges the 31 U.S.C. Chapter 38 (Administrative Remedies for False Claims and Statements) applies to the Contractor's action pertaining to this contract

1.5 Clean Air Act

1.5.1 The Contractor agrees to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act, as amended, 42 U.S.C. § 7401 et seq.

1.5.2 The Contractor agrees to report each violation to the (name of applicant entering into the contract) and understands and agrees that the (name of the applicant entering into the contract) will, in turn, report each violation as required to assure notification to the Federal Emergency Management Agency, and the appropriate Environmental Protection Agency Regional Office.

1.5.3 The Contractor agrees to include these requirements in each subcontract exceeding $150,000 financed in whole or in part with Federal assistance provided by FEMA.

1.6 Federal Water Pollution Control Act

1.6.1 The Contractor agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Federal Water Pollution Control Act, as amended, 33 U.S.C. 1251 et seq.

1.6.2 The Contractor agrees to report each violation to the (name of the applicant entering into the contract) and understands and agrees that the (name of the applicant entering into the contract) will, in turn, report each violation as required to assure notification to the Federal Emergency Management Agency, and the appropriate Environmental Protection Agency Regional Office.

1.6.3 The Contractor agrees to include these requirements in each subcontract exceeding $150,000 financed in whole or in part with Federal assistance provided by FEMA.

1.7 Debarment and Suspension

1.7.3 This contract is a covered transaction for purposes of 2 C.F.R. pt. 180 and 2 C.F.R. pt. 3000. As such, the Contractor is required to verify that none of the Contractor's principals (defined at 2 C.F.R. § 180.995) or its affiliates (defined at 2 C.F.R. § 180.905) are excluded (defined at 2 C.F.R. § 180.940) or disqualified (defined at 2 C.F.R. § 180.935).

1.7.4 The Contractor must comply with 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C, and must include a requirement to comply with these regulations in any lower tier covered transaction it enters into.

1.7.5 This certification is a material representation of fact relied upon by (insert name of recipient/subrecipient/applicant). If it is later determined that the Contractor did not comply with 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C, in addition to remedies available to (insert name of recipient/subrecipient/applicant), the Federal Government may pursue available remedies, including but not limited to suspension and/or debarment.

1.7.6 The bidder or proposer agrees to comply with the requirements of 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C while this offer is valid and throughout the period of any contract that may arise from this offer. The bidder or proposer further agrees to include a provision requiring such compliance in its lower tier covered transactions.

1.8 Byrd Anti-Lobbying Amendment, 31 U.S.C. § 1352 (as amended)

1.8.3 Contractor who apply or bid for an award of $100,000 or more shall file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, officer or employee of Congress, or an employee of a Member of Congress in connection with obtaining any Federal contract, grant, or any other award covered by 31 U.S.C. § 1352. Each tier shall also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the recipient who in turn will forward the certification(s) to the awarding agency.

1.9 PROCUREMENT OF RECOVERED MATERIALS

1.9.3 In the performance of this contract, the Contractor shall make maximum use of products containing recovered materials that are EPA-designated items unless the product cannot be acquired—

1.9.3.1 Information about this requirement, along with the list of EPA- designated items, is available at EPA's Comprehensive Procurement Guidelines web site: https://www.epa.gov/smm/comprehensive- procurement-guideline-cpg-program.

1.9.4 The Contractor also agrees to comply with all other applicable requirements of Section 6002 of the Solid Waste Disposal Act.

1.9.4.1 Competitively within a timeframe providing for compliance with the contract performance schedule;

1.9.4.2 Meeting contract performance requirements; or

1.9.4.3 At a reasonable price.

CERTIFICATION REGARDING LOBBYING (44 C.F.R. PART 18)

Certification for Contracts, Grants, Loans, and Cooperative Agreements
The undersigned certifies, to the best of his or her knowledge and belief, that:

1. No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

2. If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, “Disclosure Form to Report Lobbying,” in accordance with its instructions.

3. The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by section 1352, title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

The Contractor certifies or affirms the truthfulness and accuracy of each statement of its certification and disclosure, if any. In addition, the Contractor understands and agrees that the provisions of 31 U.S.C. Chap. 38, Administrative Remedies for False Claims and Statements, apply to this certification and disclosure, if any.

_____
Signature of Contractor’s Authorized Official

_____
Name and Title of Contractor’s Authorized Official

_____
Date

Exhibit E – Special Conditions for Security of Confidential Information

(if applicable)

If the Scope of Work or project results in additional legal and regulatory requirements regarding security of Confidential Information, those requirements regarding the use and disposition of the information, will be provided by the funding State agency in Exhibit E. (Please see section 8.E of Exhibit C.)

1. Pursuant to Exhibit C, Section 8. Confidential Information, paragraph A, the Parties shall comply with California Civil Code Sections 1798, et seq., regulations identified in Exhibit E1, when applicable and other relevant State or Federal statutes and regulations in safeguarding restricted or protected information or data which comes into their possession under this Agreement in perpetuity, and shall not use, release or publish any such information or data except as allowed in this Agreement or as permitted by law.

2. Pursuant to Exhibit C, Section 17. Right to Publish, paragraph B, the University will provide publications, presentations and other public releases resulting from work performed under this Agreement to the State for review at least thirty (30) calendar days prior to publication and will identify the proposed recipient(s). Within the review period, the State may provide feedback to the University. If the State's review of publications, presentations and other public releases resulting from work performed under this Agreement identifies Confidential Information, as defined in any Exhibit in this Agreement or by any other relevant State or Federal statutes and regulations, the University will remove any such material prior to publication.

3. The University shall not publish restricted data that is identified as such on Exhibit A4 of this Agreement, except as otherwise required by law. The obligations of this Exhibit E shall remain in perpetuity until or unless the statutes (Exhibit E1) are altered or changed.

EXHIBIT E1 - CDPH CONFIDENTIALITY STATUTES (rev. 3-2019)

Type of information:	Statutes that make it confidential:
"Personal information" meaning any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual.	California Information Practices Act (Civil Code §1798 et. seq.); Federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 USC §1320d-2(a)(2), and federal regulations in Title 45 Code of Federal Regulations §160.100 et. seq.
Medical Information	Confidentiality of Medical Information Act (CMIA), Civil Code §56.10, et seq.
Immunization information	Health and Safety Code (H&SC) §120440(d)-(h)
Information related to "special investigations" of morbidity and mortality	H&SC §100330
HIV/AIDS • Mandated Testing • Co-morbidity with other STD's • ADAP Program • PreP Program	H&SC §§121025-121035 (AIDS Public Health Records Confidentiality Act), and see also H&SC§§ 120820, 120975, 120980, 121015, 121022, 121023, 121075-121125 (AIDS Research Confidentiality Act), 121362 (confidentiality of HIV test results in connection with reports on tuberculosis patients) and 123148. H&SC §120970(i) ADAP and H&SC §120972 PrEP Other statutes apply in criminal cases and in first responder situations.
Hereditary Disorder information	H&SC §124980 (j)
Umbilical Cord Blood	H&SC §124991 (b)(1) and (g),
Prenatal rhesus(Rh)and Hepatitis B results	H&SC §125105
Genetic disease surveillance/reporting	H&SC §124975 et seq
Electronically collected personal information	Gov. Code §11015.5
Interviews, written reports, and statements procured in connection with special morbidity and mortality studies	H&SC §100330
California Cancer Registry (CCR) data	H&SC §§103875, 103885, and 100330

California Supplemental Nutrition Program for Women, Infants, and Children (WIC) Program participation	**Federal Regulations at 7 CFR §246.26(d)**
Vital Records, including Birth, Death and Marriage	**H&SC §§102230(a)(2), 102425(b), 102425.2, 102426(b), 102430, 102455, 102460, 102465, and 103025**
Childhood Lead Poisoning Prevention	**H&SC §124130**
Occupational Lead	**H&SC §124130**
California Environmental Contaminant Biomonitoring Program	**H&SC §§105440-105459**
Sexually Transmitted Diseases	**H&SC §120705 (prenatal blood tests)**
Tuberculosis	**H&SC §121362 Confidentiality of HIV test results in connection with reports on tuberculosis patients.**
Birth Defects Monitoring Program information	**H&SC §103850**
Parkinson's Disease Registry information	**H&SC §103865**
Medical Marijuana ID Program patient information	**H&SC §11362.713 (patients' and their primary caregivers' identifying information are deemed "medical information" within the meaning of the Medical Information Act)**
Cannabis–California Track-and-Trace (CCTT)	**B&PC §26067 (information for purposes of the CCTT are confidential and shall not be disclosed for purposes of the Public Records Act except as necessary for city, county, or State employees to perform official duties)**
Food and Drug Trade Secrets	**H&SC §§110165, 110370, 111792**
Food and Drug STAKE (Tobacco distributor, dealers cigarette vending locations lists)	**B&PC §22954**
LFS - Laboratory and Medical Records	**B&PC §1265(j)(2)(D)**
LFS - Human Whole Blood and Human Blood Derivatives	**H&SC §1603.1(b)(2)(b)-(e), HSC §1603.1(k)**

***This is not a comprehensive list.**

Exhibit F
Information Privacy and Security Requirements
(For Non-HIPAA/HITECH Act Contracts)

This Information Privacy and Security Requirements Exhibit (For Non-HIPAA/HITECH Act Contracts) (hereinafter referred to as "this Exhibit") sets forth the information privacy and security requirements Contractor is obligated to follow with respect to all personal and confidential information (as defined herein) disclosed to Contractor, or collected, created, maintained, stored, transmitted or used by Contractor for or on **behalf** of the California Department of Public Health (hereinafter "CDPH"), pursuant to Contractor's agreement with CDPH. (Such personal and confidential information is referred to herein collectively as "CDPH PCI".) CDPH and Contractor desire to protect the privacy and provide for the security of CDPH PCI pursuant to this Exhibit and in compliance with state and federal laws applicable to the CDPH PCI.

I. Order of Precedence: With respect to information privacy and security requirements for all CDPH PCI, the terms and conditions of this Exhibit shall take precedence over any conflicting terms or conditions set forth in any other part of the agreement between Contractor and CDPH, including Exhibit A (Scope of Work), all other exhibits and any other attachments, and shall prevail over any such conflicting terms or conditions.

II. Effect on lower tier transactions: The terms of this Exhibit shall apply to all contracts, subcontracts, and subawards, and the information privacy and security requirements Contractor is obligated to follow with respect to CDPH PCI disclosed to Contractor, or collected, created, maintained, stored, transmitted or used by Contractor for or on behalf of CDPH, pursuant to Contractor's agreement with CDPH. When applicable the Contractor shall incorporate the relevant provisions of this Exhibit into each subcontract or subaward to its agents, subcontractors, or independent consultants.

III. Definitions: For purposes of the agreement between Contractor and CDPH, including this Exhibit, the following definitions shall apply:

A. Breach:

"Breach" means:

1. the unauthorized acquisition, access, use, or disclosure of CDPH PCI in a manner which compromises the security, confidentiality or integrity of the information; or

2. the same as the definition of "breach of the security of the system" set forth in California Civil Code section 1798.29(f).

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

1. does not meet the definition of "public records" set forth in California Government Code section 6252(e), or is exempt from disclosure under any of the provisions of Section 6250, et seq. of the California Government Code or any other applicable state or federal laws; or

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

Exhibit F
Information Privacy and Security Requirements
(For Non-HIPAA/HITECH Act Contracts)

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

D. PCI: "PCI" means "personal information" and "confidential information" (as these terms are defined herein:

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

1. directly or indirectly collectively identifies or uniquely describes an individual; or

2. 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

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

4. is one of the data elements set forth in California Civil Code section 1798.29, subdivision (g)(1) or (g)(2); or

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

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

7. is protected from disclosure under applicable state or federal law.

F. Security Incident: "Security Incident" means:

1. an attempted breach; or

2. the attempted or successful unauthorized access or disclosure, modification or destruction of CDPH PCI, in violation of any state or federal law or in a manner not permitted under the agreement between Contractor and CDPH, including this Exhibit; or

3. the attempted or successful modification or destruction of, or interference with, Contractor's system operations in an information technology system, that negatively impacts the confidentiality, availability or integrity of CDPH PCI; or

4. any event that is reasonably believed to have compromised the confidentiality, integrity, or availability of an information asset, system, process, data storage, or transmission. Furthermore, an information security incident may also include an event that constitutes a violation or imminent threat of violation of information security policies or procedures, including acceptable use policies.

G. Use: "Use" means the sharing, employment, application, utilization, examination, reidentifcation, association, or analysis of information.

Exhibit F
Information Privacy and Security Requirements
(For Non-HIPAA/HITECH Act Contracts)

IV. Disclosure Restrictions: The Contractor and its employees, agents, and subcontractors shall protect from unauthorized disclosure any CDPH PCI. The Contractor shall not disclose, except as otherwise specifically permitted by the agreement between Contractor and CDPH (including this Exhibit), any CDPH PCI to anyone other than CDPH personnel or programs without prior written authorization from the CDPH Program Contract Manager, except if disclosure is required by State or Federal law.

V. Use Restrictions: The Contractor and its employees, agents, and subcontractors shall not use any CDPH PCI for any purpose other than performing the Contractor's obligations under its agreement with CDPH.

VI. Safeguards: The Contractor shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the privacy, confidentiality, security, integrity, and availability of CDPH PCI, including electronic or computerized CDPH PCI. At each location wher CDPH PCI exists under Contractor's control, the Contractor 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 the Contractor's operations and the nature and scope of its activities in performing its agreement with CDPH, including this Exhibit, and which incorporates the requirements of Section VII, Security, below. Contractor shall provide CDPH with Contractor's current and updated policies within five (5) business days of a request by CDPH for the policies.

VII. Notice and Consent: CDPH and Contractor agree to notify, obtain consent from individuals for the use and disclosure of such individuals' CDPH PCI, and document such consent. Direct interaction and consent may be oral, digital, or written. CDPH and Contractor agree to comply with Civil Code section 1798.17.

VIII. Security: The Contractor shall take any and all steps reasonably necessary to ensure the continuous security of all computerized data systems containing CDPH PCI. These steps shall include, at a minimum, complying with all of the data system security precautions listed in the Contractor Data Security Standards set forth in Attachment 1 to this Exhibit.

IX. Security Officer: At each place where CDPH PCI is located, the Contractor shall designate a Security Officer to oversee its compliance with this Exhibit and to communicate with CDPH on matters concerning this Exhibit.

X. Training: The Contractor shall provide training on its obligations under this Exhibit, at its own expense, to all of its employees who assist in the performance of Contractor's obligations under Contractor's agreement with CDPH, including this Exhibit, or otherwise use or disclose CDPH PCI.

A. The Contractor 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. The Contractor shall retain each employee's certifications for CDPH inspection for a period of three years following contract termination or completion.

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

Exhibit F
Information Privacy and Security Requirements
(For Non-HIPAA/HITECH Act Contracts)

XI. Employee Discipline: Contractor shall impose discipline that it deems appropriate (in its sole discretion) on such employees and other Contractor workforce members under Contractor's direct control who intentionally or negligently violate any provisions of this Exhibit.

Exhibit F
Information Privacy and Security Requirements
(For Non-HIPAA/HITECH Act Contracts)

XII. Breach and Security Incident Responsibilities:

A. Notification to CDPH of Breach or Security Incident: The Contractor shall notify CDPH **immediately by telephone call plus email or fax** upon the discovery of a breach (as defined in this Exhibit), **and** within **twenty-four (24) hours by email or fax** of the discovery of any security incident (as defined in this Exhibit), 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 XII(F), below. If the breach or security incident is discovered after business hours or on a weekend or holiday and involves CDPH PCI in electronic or computerized form, notification to CDPH shall be provided by calling the CDPH Information Security Office at the telephone numberslisted in Section XII(F), below. For purposes of this Section, breaches and security incidents shall be treated as discovered by Contractor as of the first day on which such breach or security incident is known to the Contractor, or, by exercising reasonable diligence would have been known to the Contractor. Contractor 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 a employee or agent of the Contractor.

Contractor shall take:

1. prompt corrective action to mitigate any risks or damages involved with the breach or security incident and to protect the operating environment; and

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

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

1. what data elements were involved and the extent of the data disclosure or access involved in the breach, including, specifically, the number of individuals whose personal information was breached; and

2. a description of the unauthorized persons known or reasonably believed to have improperly used the CDPH PCI and/or a description of the unauthorized persons known or reasonably believed to have improperly accessed or acquired the CDPH PCI, or to whom it is known or reasonably believed to have had the CDPH PCI improperly disclosed to them; and

3. a description of where the CDPH PCI is believed to have been improperly used or disclosed; and

Exhibit F
Information Privacy and Security Requirements
(For Non-HIPAA/HITECH Act Contracts)

4. a description of the probable and proximate causes of the breach or security incident; and

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

C. Written Report: The Contractor 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 Contractor is considered only a custodian and/or non-owner of the CDPH PCI, Contractor shall, at its sole expense, and at the sole election of CDPH, either:

1. 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. Contractor 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

2. 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 California Civil Code section 1798.29, and regardless of whether Contractor is considered only a custodian and/or non-owner of the CDPH PCI, Contractor shall, at its sole expense, and at the sole election of CDPH, either:

1. 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). Contractor 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

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

F. CDPH Contact Information: To direct communications to the above referenced CDPH staff, the Contractor shall initiate contact as indicated herein. CDPH reserves the right to make changes to the contact information below by verbal or written notice to the Contractor. Said changes shall not require an amendment to this Exhibit or the agreement to which it is incorporated.

Exhibit F
Information Privacy and Security Requirements
(For Non-HIPAA/HITECH Act Contracts)

CDPH Program Contract Manager	**CDPH Privacy Officer**	**CDPH Chief Information Security Officer**
See the Scope of Work exhibit for Program Contract Manager	Privacy Officer Privacy Office Office of Legal Services California Dept. of Public Health 1415 L Street, 5th Floor Sacramento, CA 95814 Email: privacy@cdph.ca.gov Telephone: (877) 421-9634	Chief Information Security Officer Information Security Office California Dept. of Public Health P.O. Box 997377 MS6302 Sacramento, CA 95899-7413 Email: cdphiso@cdph.ca.gov Telephone: (855) 500-0016

XIII. Documentation of Disclosures for Requests for Accounting: Contractor shall document and make available to CDPH or (at the direction of CDPH) to an Individual such disclosures of CDPH PCI, 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.

XIV. Requests for CDPH PCI by Third Parties: The Contractor and its employees, agents, or subcontractors shall promptly transmit to the CDPH Program Contract Manager all requests for disclosure of any CDPH PCI requested by third parties to the agreement between Contractor 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. CDPH PCI shall only be shared with law enforcement pursuant to a valid court order.

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

XVI. Return or Destruction of CDPH PCI on Expiration or Termination: Upon expiration or termination of the agreement between Contractor and CDPH for any reason, Contractor shall securely return or destroy the CDPH PCI. If return or destruction is not feasible, Contractor shall provide a written explanation to the CDPH Program Contract Manager, the CDPH Privacy Officer and the CDPH Chief Information Security Officer, using the contact information listed in Section XII(F), above.

A. Retention Required by Law: If required by state or federal law, Contractor may retain, after expiration or termination, CDPH PCI for the time specified as necessary to comply with the law.

B. Obligations Continue Until Return or Destruction: Contractor's obligations under this Exhibit shall continue until Contractor returns or destroys the CDPH PCI or returns the CDPH PCI to CDPH; provided however, that on expiration or termination of the agreement between Contractor and CDPH, Contractor shall not further use or disclose the CDPH PCI except as required by state or federal law.

Exhibit F
Information Privacy and Security Requirements
(For Non-HIPAA/HITECH Act Contracts)

C. Notification of Election to Destroy CDPH PCI: If Contractor elects to destroy the CDPH PCI, Contractor shall certify in writing, to the CDPH Program Contract Manager, the CDPH Privacy Officer and the CDPH Chief Information Security Officer, using the contact information listed in Section XI(F), above, that the CDPH PCI has been securely destroyed. The notice shall include the date and type of destruction method used.

XVII. Amendment: The parties acknowledge that federal and state laws regarding information security and privacy rapidly evolves and that amendment of this Exhibit 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 CDPH PCI.The parties agree to promptly enter into negotiations concerning an amendment to this Exhibit consistent with new standards and requirements imposed by applicable laws and regulations.

XVIII. Assistance in Litigation or Administrative Proceedings: Contractor shall make itself and any subcontractors, workforce employees or agents assisting Contractor in the performance of its obligations under the agreement between Contractor 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 the Contractor, except where Contractor or its subcontractor, workforce employee or agent is a named adverse party.

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

XX. Interpretation: The terms and conditions in this Exhibit 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 Exhibit shall be resolved in favor of a meaning that complies and is consistent with federal and state laws and regulations.

XXI. Survival: If Contractor does not return or destroy the CDPH PCI upon the completion or termination of the Agreement, the respective rights and obligations of Contractor under Sections VI, VIII and XII of this Exhibit shall survive the completion or termination of the agreement between Contractor and CDPH.

Exhibit F
Information Privacy and Security Requirements
(For Non-HIPAA/HITECH Act Contracts)

Attachment 1
Contractor Data Security Standards

1. General Security Controls

A. ***Confidentiality Statement.*** All persons that will be working with CDPH PCI must sign a confidentiality statement. The statement must include at a minimum, General Use, Security and Privacy safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to CDPH PCI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for CDPH inspection for a period of three (3) years following contract termination.

B. ***Background check.*** Before a member of the Contractor's workforce may access CDPH PCI, Contractor must conduct a thorough background check of that worker and evaluate the results to assure that there is no indication that the worker may present a risk for theft of confidential data. The Contractor shall retain each workforce member's background check documentation for a period of three (3) years following contract termination.

C. ***Workstation/Laptop encryption.*** All workstations and laptops that process and/or store CDPH PCI must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher. The encryption solution must be full disk unless approved by the CDPH Information Security Office.

D. ***Server Security.*** Servers containing unencrypted CDPH PCI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

E. ***Minimum Necessary.*** Only the minimum necessary amount of CDPH PCI required to perform necessary business functions may be copied, downloaded, or exported.

F. ***Removable media devices.*** All electronic files that contain CDPH PCI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, smart devices tapes etc.). PCI must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher

G. ***Antivirus software.*** All workstations, laptops and other systems that process and/or store CDPH PCI must install and actively use a comprehensive anti-virus software solution with automatic updates scheduled at least daily.

H. ***Patch Management.*** All workstations, laptops and other systems that process and/or store CDPH PCI must have operating system and application security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release.

I. ***User IDs and Password Controls.*** All users must be issued a unique user name for accessing CDPH PCI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password.

Exhibit F
Information Privacy and Security Requirements
(For Non-HIPAA/HITECH Act Contracts)

Passwords are not to be shared. Must be at least eight characters. Must be a non-dictionary word. Must not be stored in readable format on the computer. Must be changed every 60 days. Must be changed if revealed or compromised. Must be composed of characters from at least three of the following four groups from the standard keyboard:

- Upper case letters (A-Z)
- Lower case letters (a-z)
- Arabic numerals (0-9)
- Non-alphanumeric characters (punctuation symbols)

J. ***Data Sanitization.*** All CDPH PCI must be sanitized using NIST Special Publication 800-88 standard methods for data sanitization when the CDPH PCI is no longer needed.

2. System Security Controls

A. ***System Timeout.*** The system must provide an automatic timeout, requiring reauthentication of the user session after no more than 20 minutes of inactivity.

B. ***Warning Banners.*** All systems containing CDPH PCI must display a warning banner each time a user attempts access, stating that data is confidential, systems are logged, and system use is for business purposes only. User must be directed to log off the system if they do not agree with these requirements.

C. ***System Logging.*** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for CDPH PCI, or which alters CDPH PCI. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users This logging must be included for all user privilege levels including, but not limited to, systems administrators. If CDPH PCI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.

D. ***Access Controls.*** The system must use role based access controls for all user authentications, enforcing the principle of least privilege.

E. ***Transmission encryption.*** All data transmissions of CDPH PCI outside the contractor's secure internal network must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher. Encryption can be end to end at the network level, or the data files containing CDPH PCI can be encrypted. This requirement pertains to any type of CDPH PCI in motion such as website access, file transfer, and E-Mail.

F. ***Intrusion Detection***. All systems involved in accessing, holding, transporting, and protecting CDPH PCI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

3. Audit Controls

Exhibit F
Information Privacy and Security Requirements
(For Non-HIPAA/HITECH Act Contracts)

A. ***System Security Review.*** All systems processing and/or storing CDPH PCI must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews shall include vulnerability scanning tools.

B. ***Log Reviews.*** All systems processing and/or storing CDPH PCI must have a routine procedure in place to review system logs for unauthorized access.

C. ***Change Control.*** All systems processing and/or storing CDPH PCI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

4. Business Continuity / Disaster Recovery Controls

A. ***Disaster Recovery.*** Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic CDPH PCI in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this agreement for more than 24 hours.

B. ***Data Backup Plan.*** Contractor must have established documented procedures to securely backup CDPH PCI to maintain retrievable exact copies of CDPH PCI. The backups shall be encrypted.The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and the amount of time to restore CDPH PCI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of CDPH data.

5. Paper Document Controls

A. ***Supervision of Data.*** CDPH PCI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. CDPH PCI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

B. ***Escorting Visitors.*** Visitors to areas where CDPH PCI is contained shall be escorted and CDPH PHI shall be kept out of sight while visitors are in the area.

C. ***Confidential Destruction.*** CDPH PCI must be disposed of through confidential means, using NIST Special Publication 800-88 standard methods for data sanitization when the CDPH PSCI is no longer needed.

D. ***Removal of Data.*** CDPH PCI must not be removed from the premises of the Contractor except with express written permission of CDPH.

E. ***Faxing.*** Faxes containing CDPH PCI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving

Exhibit F
Information Privacy and Security Requirements
(For Non-HIPAA/HITECH Act Contracts)

faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending.

F. ***Mailing.*** CDPH PCI shall only be mailed using secure methods. Large volume mailings of CDPH PHI shall be by a secure, bonded courier with signature required on receipt. Disks and other transportable media sent through the mail must be encrypted with a CDPH approved solution, such as a solution using a vendor product specified on the CALIFORNIA STRATEGIC SOURCING INITIATIVE.