

THE INFORMATION IN THIS BOX IS NOT A PART OF THE CONTRACT AND IS FOR COUNTY USE ONLY



Contract Number  
22-795 A-2

SAP Number




### Department of Public Health

<b>Department Contract Representative</b>	<u>Laura Edwards</u>
<b>Telephone Number</b>	<u>909-677-3929</u>
<b>Contractor</b>	<u>California Department of Public Health</u>
<b>Contractor Representative</b>	<u>Contract and Procurement Support Unit</u>
<b>Telephone Number</b>	<u>(916) 928-8500</u>
<b>Contract Term</b>	<u>10/1/2022 through 9/30/2025</u>
<b>Original Contract Amount</b>	<u>\$41,727,837</u>
<b>Amendment Amount</b>	<u>\$13,464</u>
<b>Total Contract Amount</b>	<u>\$41,741,301</u>
<b>Cost Center</b>	<u>9300061000</u>

**Briefly describe the general nature of the contract:**

Approve Amendment No. 2 to Agreement No. 22-795 (State Agreement No. 22-10281) with the California Department of Public Health, for the Women, Infants and Children Nutrition Program, increasing the grant amount by \$13,464, from \$41,727,837 to \$41,741,301, with no change to the period of October 1, 2022 through September 30, 2025.

**FOR COUNTY USE ONLY**

Approved as to Legal Form	Reviewed for Contract Compliance	Reviewed/Approved by Department
 Adam Ebright, Deputy County Counsel		 <small>Joshua Dugas (Sep 7, 2023 11:31 PDT)</small> Joshua Dugas, Director
Date <u>Sep 7, 2023</u>	Date _____	Date <u>Sep 7, 2023</u>



TOMÁS J. ARAGÓN, MD, DrPH  
Director and State Public Health Officer

State of California—Health and Human Services Agency  
California Department of Public Health



GAVIN NEWSOM  
Governor

**Date:** July 24, 2023

**TO:** San Bernardino County

**FROM:** California Department of Public Health (CDPH)

**SUBJECT:** Contract # 22-10281 A01

Please find the above-referenced Contract Agreement between the California Department of Public Health and San Bernardino County, attached for your review and signature.

**IMPORTANT:** The Agreement is an Adobe Acrobat PDF document with "READ ONLY" attributes. Please do not alter this Agreement for any reason. If you encounter any problems or find that a correction is needed, please contact your Contract Manager immediately.

To approve this Agreement, submit one (1) electronic copy (**do not mail in hard copies**) of each document listed below to the following mailbox: [LocalContracts@cdph.ca.gov](mailto:LocalContracts@cdph.ca.gov). Please title the email Subject line: Signed Agreement for 22-10281 A01 (San Bernardino).

- One (1) signed copy of the Standard Agreement - Amendment (STD 213A). This document can be signed electronically or physically signed, scanned and returned via email.
- One (1) signed copy of the Board Resolution/Order/Motion, ordinance or other similar document authorizing execution of the Agreement and any signatory designees.
- One (1) signed copy of the Contractor's current insurance policy certificates and endorsements.

In an effort to expedite this Contract Agreement through the approval process, we request that the items listed above be returned no later than **three weeks from the date of this letter**, in order to avoid disruption in services. Failure to sign and submit the required forms by the date indicated will result in delayed approval of your Agreement.

Please contact your Contract Manager if you have any questions or will need additional time to return the signed documents.



CDPH Women, Infants and Children (WIC) Division  
3901 Lennane Drive, MS 8600, Sacramento, CA 95834  
P.O. Box 997375, MS 8600, Sacramento, CA 95899-7375  
(916) 928-8500 | [www.wicworks.ca.gov](http://www.wicworks.ca.gov)



San Bernardino County  
Page 2  
July 24, 2023

Thank you,

*Contract and Procurement Support Unit*

Attachments

CONFIDENTIALITY NOTICE: This communication along with its contents may contain confidential and/or legally privileged information. It is solely for the use of the intended recipient(s). Unauthorized interception, review, use or disclosure is prohibited and may violate applicable laws including the Electronic Communications Privacy Act. If you are not the intended recipient, please contact the sender and destroy all copies of the communication.

STD 213A (Rev. 4/2020)

<input checked="" type="checkbox"/> CHECK HERE IF ADDITIONAL PAGES ARE ATTACHED <u>2</u> PAGES	AGREEMENT NUMBER <b>22-10281</b>	AMENDMENT NUMBER <b>A01</b>	Purchasing Authority Number
------------------------------------------------------------------------------------------------	-------------------------------------	--------------------------------	-----------------------------

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

CONTRACTING AGENCY NAME

California Department of Public Health

CONTRACTOR NAME

San Bernardino County

2. The term of this Agreement is:

START DATE

October 1, 2022

THROUGH END DATE

September 30, 2025

3. The maximum amount of this Agreement after this Amendment is:

\$ 41,741,301.00 Forty-One Million Seven Hundred Forty-One Thousand Three Hundred One Dollars

4. The parties mutually agree to this amendment as follows. All actions noted below are by this reference made a part of the Agreement and incorporated herein:

1. This amendment increases the contract by \$13,464.00, changing the total amount to read \$41,741,301.00, to better support the Contractor's needs, and is shifting funds in fiscal years 1, 2 and 3 to accommodate anticipated expenses.

All other terms and conditions shall remain the same.

IN WITNESS WHEREOF, THIS AGREEMENT HAS BEEN EXECUTED BY THE PARTIES HERETO.

**CONTRACTOR**

CONTRACTOR NAME (if other than an individual, state whether a corporation, partnership, etc.)

San Bernardino County

CONTRACTOR BUSINESS ADDRESS

351 North Mountain View Avenue

CITY

San Bernardino

STATE

CA

ZIP

92415

PRINTED NAME OF PERSON SIGNING

Dawn Rowe

TITLE

Chair, Board of Supervisors

CONTRACTOR AUTHORIZED SIGNATURE

*Dawn Rowe*

DATE SIGNED

SEP 12 2023

**STATE OF CALIFORNIA**

CONTRACTING AGENCY NAME

California Department of Public Health

CONTRACTING AGENCY ADDRESS

1616 Capitol Avenue, Suite 74.262, MS 1802, PO Box 997377

CITY

Sacramento

STATE

CA

ZIP

95899

PRINTED NAME OF PERSON SIGNING

Joseph Torrez

TITLE

Chief, Contracts Management Unit

CONTRACTING AGENCY AUTHORIZED SIGNATURE

DATE SIGNED

CALIFORNIA DEPARTMENT OF GENERAL SERVICES APPROVAL

EXEMPTION (If Applicable)

SIGNED AND CERTIFIED THAT A COPY OF THIS DOCUMENT HAS BEEN DELIVERED TO THE CHAIRMAN OF THE BOARD  
 LYNN MONELL  
 Clerk of the Board of Supervisors of the County of San Bernardino

By \_\_\_\_\_



II. Exhibit A, Scope of Work, Provision 4 has been revised as follows:

**4. Project Representatives**

A. The project representatives during the term of this agreement will be:

California Department of Public Health	San Bernardino County
Meghann Schiveley <u>Harrison</u> , Contract Manager Telephone: 916-928-8577 E-mail: <del>Meghann.schiveley@cdph.ca.gov</del> <b>Meghann.harrison@cdph.ca.gov</b>	Joshua Dugas, MBA, REHS, Director of Public Health Telephone: 909-387-9146 E-mail: Joshua.dugas@dph.sbcounty.gov

B. Direct all inquiries to:

California Department of Public Health	San Bernardino County
CDPH/WIC Division Attention: Meghann Schiveley <u>Harrison</u> , Contract Manager Local Services Branch 3901 Lennane Drive Sacramento, CA 95834  Telephone: 916-928-8577 E-mail: <del>Meghann.schiveley@cdph.ca.gov</del> <b>Meghann.harrison@cdph.ca.gov</b>	Attention: Heather Wellons-Blum, Program Manager, Registered Dietitian 1505 S. D Street, Suite 203 San Bernardino, CA 92408  Telephone: <del>909-388-5669</del> <b>909-388-5663</b> E-mail: hblum-wellons@dph.sbcounty.gov

C. All payments from CDPH to the Contractor; shall be sent to the following address:

Remittance Address
Federal ID #: 95-6002748
FI\$CAL ID #:
Contractor: San Bernardino County
Attention: Cashier
Address: <del>351 North Mountain View Ave, San Bernardino, CA 92415-0010</del> <b>451 E. Vanderbilt Way, STE 200, San Bernardino, CA 92408</b>
Contract Number: 22-10281 <b>A01</b>
Email: Eric.Patrick@dph.sbcounty.gov

D. Either party may make changes to the information above by giving written notice to the other party. Said changes shall not require an amendment to this agreement but will require a new CDPH 9083 Governmental Entity Taxpayer ID Form or STD 204 Payee Data Record form. The completed form must be submitted to the Contract Manager for processing.

III. Exhibit A, Scope of Work, Provision 8.12) has been revised to include the following:

**e) Continuous Time Reporting - Books for Kids Program (if applicable)**

**The Contractor shall adhere to all fiscal procedures required for Books for Kids restricted funds and keep continuous time reports for all dual funded positions performing Books for Kids related duties as outlined in Exhibit A, Provision 8.26).**

IV. Exhibit A, Scope of Work, Provision 8 has been revised to include the following:

**26) Books for Kids Program (only applies to the Contractor that receives funds for this project)**

**The Contractor will assure that the funding is spent on books for WIC participants 0-5 years old. Local agencies may subcontract the activity to another entity to purchase and distribute books for eligible WIC participants only. When subcontracting to another entity, data must be obtained and made available, that identifies the number of WIC participants who receive the books and the number of books distributed by language.**

V. Exhibit B, Budget Detail and Payment Provisions has been replaced in its entirety.

VI. Exhibit B, Attachment I, Budget Detail has been replaced in its entirety.

VII. Exhibit B, Attachment II, Facility Costs has been replaced in its entirety.

VIII. Exhibit G, Information Privacy and Security Requirements (For CDPH WIC Contracts) has been replaced in its entirety.



Exhibit B Attachment II  
Facility Costs  
October 1, 2022 - September 30, 2025

Site Street Address, City, State & Zip Code	Type of Space (e.g., Clinic, Admin, Training, Storage)	Total Square Footage	Year 1		Year 2		Year 3		Year 1 Total	Year 2 Total	Year 3 Total	Amended Total
			Total Cost of Site Per Month	Amended Total Site Cost Per Year	Total Cost of Site Per Month	Amended Total Site Cost Per Year	Total Cost of Site Per Month	Amended Total Site Cost Per Year				
<b>Total Facility Costs:</b>				\$ 1,672,092	\$ 1,740,384				\$ 1,700,734	\$ 1,886,864	\$ 1,728,966	\$ 1,714,356
2035 N D St, San Bernardino, CA 92405	Clinic Site	4700	8,518	102,219	103,032	8,837	104,244	8,850	105,950	106,320	106,320	168,036
6507 Arrow Rte, Box 7, Site A Rancho Cucamonga, 91730	Clinic Site	3700	8,235	96,850	107,220	8,399	100,798	8,399	100,798	102,792	102,792	100,798
850 E Foothill Blvd, Rialto, 92376	Clinic Site	3914	6,120	73,440	73,440	6,241	74,892	6,366	76,398	78,390	78,390	78,390
2527 Desert Queen Ave, Twentynine Palms, 92277	Clinic Site	3214	5,254	63,048	48,312	5,311	63,732	5,370	64,596	66,440	66,440	49,716
1596 South D Street, San Bernardino, 92415	Administrative Site	9374	19,043	228,516	228,516	19,424	233,068	19,812	233,068	237,744	237,744	237,744
1515 N Riverside Ave, Rialto, 92376	Clinic Site	2769	10,002	120,024	58,462	10,112	121,344	10,224	122,688	122,688	122,688	-
699 E Mill Street, San Bernardino 92408	Clinic Site	4173	11,150	133,800	134,196	11,338	136,056	11,530	138,360	139,952	139,952	138,752
15547 11th St, 700, Victorville, 92395	Clinic Site	3963	8,796	105,192	105,192	8,839	107,256	8,917	107,256	109,404	109,404	109,404
1149 E Cooley Drive, Colton, 92324	Storage	825	182	2,184	3,024	186	2,232	189	2,268	2,298	2,298	3,072
809 E Lugona Ave, Suite K, Redlands 92374	Clinic Site	3000	5,750	69,000	69,756	5,844	70,128	5,940	71,052	71,200	71,200	72,216
322 S. Walsman Ave., San Bernardino, 92409	Storage	1910	869	10,428	10,428	869	10,428	869	10,428	10,428	10,428	10,428
1538 E Highland Ave., San Bernardino, 92404	Clinic Site	3313	8,481	101,772	104,590	8,683	103,690	8,822	105,596	106,596	106,596	106,596
9191 Sierra Ave., Suite 104, Fontaine, 92335	Clinic Site	5793	15,774	189,288	254,508	16,088	193,056	16,488	198,288	203,976	203,976	203,976
56507 Penn Trail, Yuca Valley 92594	Clinic Site	776	1,743	20,916	20,916	1,778	21,336	1,813	21,756	21,996	21,996	21,996
150 E. Holt Blvd., Ontario 91751	Clinic Site	4628	12,597	150,864	127,058	12,733	153,036	12,942	155,700	158,364	158,364	158,364
331 East Mountain View Ave., Suite A, Barstow, 92311	Clinic Site	1493	796	9,552	12,564	796	9,552	796	9,552	10,044	10,044	10,044
250 E. "O" Street, Colton, 92323	Clinic Site	2600	4,781	57,132	64,632	4,781	57,132	4,781	57,132	57,132	57,132	57,132
1620, 1317, Inver Loop & Cobstone, Room 9, Ft. Irwin, 92310	Clinic Site	1625	3,386	40,632	40,632	3,386	40,632	3,386	40,632	41,124	41,124	41,124
14135 Main Street, Hesperia, 92345	Clinic Site	4646	11,320	135,840	153,156	11,545	138,540	11,764	141,156	144,156	144,156	144,156



**Exhibit G**  
**Information Privacy and Security Requirements**  
**(For CDPH WIC Contracts)**

This Information Privacy and Security Requirements Exhibit (For CDPH WIC Contracts) ("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 ("CDPH"), pursuant to Contractor's agreement with CDPH. Such personal and confidential information is referred to herein collectively as "CDPH PCI".

CDPH administers the California Special Supplemental Nutrition Program for Women, Infants, and Children (WIC Program) pursuant to a grant from the United States Department of Agriculture (USDA), pursuant to the Child Nutrition Act of 1966, title 42 of the United States Code (U.S.C.), Section 1786 (Public law 89-645, Section 17), as amended, and in accordance with governing administration of grants (2 CFR part 200, subparts A through F and USDA implementing regulations 2 CFR part 400 and part 415); governing non-procurement debarment/suspension (2 CFR part 180, OMB Guidelines to Agencies on Government-wide Debarment and Suspension and USDA implementing regulations 2 CFR part 417); governing restrictions on lobbying (2 CFR part 200, subpart E and USDA implementing regulations 2 CFR part 400, part 415, and part 418); and governing the drug-free workplace requirements (2 CFR part 182, Government-wide Requirements for Drug-Free Workplace); FNS guidelines; and, instructions issued under the FNS Directives Management System.

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. The Contractor may enter into a data sharing agreement for CDPH PCI only when permitted under State and Federal laws and authorized in writing by the CDPH WIC Program. If the Contractor chooses to enter into a data sharing agreement, it shall be the Contractor's sole responsibility to incorporate all relevant provisions of this Exhibit into any data sharing agreement(s) the Contractor may execute.
- 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).

**Exhibit G**  
**Information Privacy and Security Requirements**  
**(For CDPH WIC Contracts)**

- B. Confidential Information: “Confidential information” means:
1. any information about a [WIC] applicant or participant, whether it is obtained from the applicant or participant, another source, or generated as a result of WIC application, certification, or participation, that individually identifies an applicant or participant and/or family member(s) as set forth in 7 Code of Federal Regulations part 246.26(d)(1)(i);
  2. any information about a [WIC] vendor (whether it is obtained from the vendor or another source) that individually identifies the vendor, except for vendor's name, address, telephone number, Web site/e-mail address, store type, and authorization status as set forth in 7 Code of Federal Regulations part 246.26(e);
  3. any information that 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
  4. any information that is contained in documents, files, folders, books or records that are clearly labeled, marked or designated with the word “confidential” by CDPH.
- 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. is about a [WIC] applicant or participant, whether it is obtained from the applicant or participant, another source, or generated as a result of WIC application, certification, or participation, that individually identifies an applicant or participant and/or family member(s) as set forth in 7 Code of Federal Regulations part 246.26(d)(1)(i); or
  4. is about a [WIC] vendor (whether it is obtained from the vendor or another source) that individually identifies the vendor, except for vendor's name, address, telephone number, Web site/e-mail address, store type, and authorization status as set forth in 7 Code of Federal Regulations part 246.26(e); or
  5. meets the definition of “personal information” set forth in California Civil Code section 1798.3, subdivision (a); or
  6. is one of the data elements set forth in California Civil Code section 1798.29, subdivision (g)(1) or (g)(2); or

**Exhibit G**  
**Information Privacy and Security Requirements**  
**(For CDPH WIC Contracts)**

7. 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
8. meets the definition of “health insurance information” set forth in California Civil Code section 1798.29, subdivision (h)(3); or
9. 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, or analysis of information.

IV. Disclosure Restrictions: The Contractor and its employees, agents, and subcontractors shall protect from unauthorized disclosure any CDPH PCI. The Contractor shall not grant access or disclose CDPH PCI to any employees, agents, and subcontractors unless CDPH WIC has determined those individuals have a need to know the CDPH PCI in order to perform Contractor’s obligations under its agreement with CDPH WIC. The Contractor shall not access or disclose any CDPH PCI to anyone other than personnel of the CDPH WIC Program or CDPH OLS without prior written authorization from the CDPH WIC Program, except if disclosure is required by State or Federal law. All disclosures must be limited to the minimum necessary, to the extent practicable, and must comply with the requirements set forth in State and Federal law, including but not limited to Civil Code 1798 et seq. (the California Information Practices Act) and 7 Code of Federal Regulations part 246.26.

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 where 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

**Exhibit G**  
**Information Privacy and Security Requirements**  
**(For CDPH WIC Contracts)**

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. 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.
- VIII. 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.
- IX. 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.
- X. 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 G**  
**Information Privacy and Security Requirements**  
**(For CDPH WIC Contracts)**

**XI. Breach and Security Incident Responsibilities:**

- A. Notification to CDPH of Breach or Security Incident: The Contractor shall notify CDPH **immediately by telephone and email** upon the discovery of a breach (as defined in this Exhibit), and **within twenty-four (24) hours by email** 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 XI(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 numbers listed in Section XI(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 an 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;
  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;
  3. a description of where the CDPH PCI is believed to have been improperly used or disclosed;
  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.

**Exhibit G**  
**Information Privacy and Security Requirements**  
**(For CDPH WIC Contracts)**

- 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 G  
 Information Privacy and Security Requirements  
 (For CDPH WIC Contracts)**

<b>CDPH Program Contract Manager</b>	<b>CDPH Privacy Officer</b>	<b>CDPH Chief Information Security Officer</b>	<b>CDPH OLS Contact for Third Party Information Requests</b>
See Scope of Work for Program Contract Manager	Privacy Officer Privacy Office c/o Office of Legal Services California Dept. of Public Health 1415 L Street, 5 <sup>th</sup> Floor, Suite 500 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 997413 MS6302 Sacramento, CA 95899-7413  Email: ICDPH.InfoSecurityOffice@cdph.ca.gov Telephone: (855) 500-0016	Assistant Chief Counsel, Public Health Programs Office of Legal Services California Dept. of Public Health 1415 L Street, 5 <sup>th</sup> Floor Sacramento, CA 95814  Telephone: (916) 558-1710

XII. 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.

XIII. Requests for CDPH PCI by Third Parties: The Contractor and its employees, agents, or subcontractors shall promptly transmit to the CDPH OLS 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.

Contractor and its employees, agents, or subcontractors shall transmit in writing to CDPH Office of Legal Services all requests for disclosure of CDPH PCI from parties other than CDPH WIC within one business day.

Subpoena, search warrant, or other litigation involved requests: **In the event that a subpoena, search warrant, or other litigation involved request for CDPH PCI is received by the Contractor, the Contractor shall immediately notify the CDPH Office of Legal Services contact by telephone call** in order to allow CDPH WIC to follow the procedures and restrictions imposed by 7 Code of Federal Regulations part 246.26(i). CDPH shall be the party with sole authority to determine whether any, and specifically what, information may be produced.

**Exhibit G**  
**Information Privacy and Security Requirements**  
**(For CDPH WIC Contracts)**

- XIV. Audits, Inspection and Enforcement: CDPH, USDA, or representatives of the Comptroller General of the United States 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.
- XV. 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 XI(F), above.
- A. Retention Required by Law: If required by state or federal law, Contractor shall retain, after expiration or termination, CDPH PCI for the time specified as necessary to comply with the law. Pursuant to 7 C.F.R. part 246.25(a)(2), if records related to the agreement between Contractor and CDPH, including CDPH PCI, is not returned to CDPH upon the termination of the agreement, all records shall be retained for a minimum of three years. If any litigation, claim, negotiation, audit or other action involving the CDPH PCI shared under this agreement has commenced before the end of the three-year period, the records shall be kept until all issues are resolved, or until the end of the regular three-year period, whichever is later. If USDA or any unit thereof deems any of the CDPH PCIs to be of historical interest, it may require the Contractor to forward such records to USDA or any unit thereof whenever the Contractor is disposing of them.
- 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.
- 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.
- XVI. 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.
- XVII. 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.



**Exhibit G**  
**Information Privacy and Security Requirements**  
**(For CDPH WIC Contracts)**

- XVIII. 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.
- XIX. Interpretation: The terms and conditions in this Exhibit shall be interpreted as broadly as necessary to implement and comply with regulations and applicable federal and 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.
- XX. 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, VII, XI, and XIII of this Exhibit shall survive the completion or termination of the agreement between Contractor and CDPH.

**Exhibit G**  
**Information Privacy and Security Requirements**  
**(For CDPH WIC Contracts)**

**Attachment 1**  
**Contractor Data Security Standards**

**I. Personnel Controls**

- A. *Workforce Members Training and Confidentiality.*** Before being allowed access to CDPH PCI, all Contractor's workforce members who will be granted access to CDPH PCI must be trained in their security and privacy roles and responsibilities at Contractor's expense and must sign a confidentiality and acceptable CDPH PCI use statement. Training must be on an annual basis. Acknowledgments of completed training and confidentiality statements, which have been signed and dated by workforce members must be retained by the Contractor for a period of three (3) years following contract termination. Contractor shall provide the acknowledgements within five (5) business days to CDPH if so requested.
- B. *Workforce Members Discipline.*** Appropriate sanctions, including termination of employment where appropriate, must be applied against workforce members who fail to comply with privacy policies and procedures, acceptable use agreements, or any other provisions of these requirements.
- C. *Workforce Member Assessment.*** Before being permitted access to CDPH PCI, Contractor must assure there is no indication workforce member may present a risk to the security or integrity of CDPH PCI. Contractor shall retain the workforce member's assessment documentation for a period of three (3) years following contract termination.

**II. Technical Security Controls**

- A. *Encryption.*** All desktop computers, mobile computing devices, and portable electronic storage media that processes or stores CDPH PCI must be encrypted using a FIPS 140-2 certified 128 bit or higher algorithm. The encryption solution must be full disk unless approved by the CDPH Information Security Office (ISO) and Privacy Office (PO). FIPS 140-2 certified 128 bit or higher algorithm end-to-end, individual file encryption, or ISO approved compensating security controls, shall be used to protect CDPH PCI transmitted or accessed outside the Contractor's secure internal network (e.g., email, remote access, file transfer, internet/website communication tools).
- B. *Server Security.*** Servers containing unencrypted CDPH PCI must have sufficient local and network perimeter administrative, physical, and technical controls in place to protect the CDPH information asset, based upon a current risk assessment/system security review.
- C. *Minimum Necessary.*** Only the minimum amount of CDPH PCI required to complete an authorized task or workflow may be copied, downloaded, or exported to any individual device.
- D. *Antivirus software.*** Contractor shall employ automatically updated malicious code protection mechanisms (anti-malware programs or other physical or software-based solutions) at its network perimeter and at workstations, servers, or mobile computing devices to continuously monitor and take actions against system or device attacks, anomalies, and suspicious or inappropriate activities.
- E. *Patch Management.*** All devices that process or store CDPH PCI must have a documented patch management process. Vulnerability patching for Common Vulnerability Scoring System (CVSS) "Critical" severity ratings (CVSS 9.0 – 10.0) shall be completed within forty-eight (48) hours of

**Exhibit G**  
**Information Privacy and Security Requirements**  
**(For CDPH WIC Contracts)**

publication or availability of [WIC] vendor supplied patch; "High" severity rated (CVSS 7.0- 8.9) shall be completed within seven (7) calendar days of publication or availability of vendor supplied patch; all other vulnerability ratings (CVSS 0.1 – 6.9) shall be completed within thirty (30) days of publication or availability of vendor supplied patch, unless prior ISO and PO variance approval is granted.

- F. *User Identification and Access Control.*** All Contractor workforce members must have a unique local and/or network user identification (ID) to access CDPH PCI. The unique ID may be passwords, physical authenticators, or biometrics, or in the case of multi-factor authentication, some combination thereof. Should a workforce member no longer be authorized to access CDPH PCI, or an ID has been compromised, that ID shall be promptly disabled or deleted. User ID's must integrate with user role-based access controls to ensure that individual access to CDPH PCI is commensurate with job-related responsibilities.
- G. *CDPH PCI Destruction.*** When no longer required for business needs or legal retention periods, all electronic and physical media holding CDPH PCI must be purged from Contractor's systems and facilities using the appropriate guidelines for each media type as described in the prevailing "National Institute of Standards and Technology – Special Publication 800-88" – "Media Sanitization Decision Matrix."
- H. *System Inactivity Timeout.*** Contractor's computing devices holding, or processing CDPH PCI must be configured to automatically log-off an authenticated user or lock the device in a manner where the user must reauthenticate the user session after no more than twenty (20) minutes of user inactivity.
- I. *Warning Banners.*** During a user log-on process, all systems providing access to CDPH PCI, must display a warning banner stating that the CDPH PCI is confidential, system and user activities are logged, and system and CDPH PCI use is for authorized business purposes only. User must be directed to log-off the system if they do not agree with these conditions.
- J. *System Logging.*** Contractor shall ensure the information systems and devices that hold or process CDPH PCI are capable of being audited and the events necessary to reconstruct transactions and support after-the-fact investigations are maintained. This includes the auditing necessary to cover related events, such as the various steps in distributed, transaction-based processes and actions in service-oriented architectures. Audit trail information with CDPH PCI must be stored with read-only permissions and be archived for three (3) years after event occurrence. There must also be a documented and routine procedure in place to review system logs for unauthorized access.
- K. *Intrusion Detection.*** All Contractor systems and devices holding, processing, or transporting CDPH PCI that interact with untrusted devices or systems via the Contractor intranet and/or the internet must be protected by a monitored comprehensive intrusion detection system and/or intrusion prevention system.

**III. Audit Controls**

- A. *System Security Review.*** Contractor, to assure that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection for CDPH PCI, shall conduct at least, an annual administrative assessment of risk, including the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or

**Exhibit G**  
**Information Privacy and Security Requirements**  
**(For CDPH WIC Contracts)**

destruction of an information system or device holding processing, or transporting CDPH PCI, along with periodic technical security reviews using vulnerability scanning tools and other appropriate technical assessments.

- B. *Change Control.*** All Contractor systems and devices holding, processing, or transporting CDPH PCI shall have a documented change control process for hardware, firmware, and software to protect the systems and assets against improper modification before, during, and after system implementation.

**IV. Business Continuity / Disaster Recovery Controls**

- A. *Emergency Mode Operation Plan.*** Contractor shall develop and maintain technical recovery and business continuity plans for systems holding, processing, or transporting CDPH PCI to ensure the continuation of critical business processes and the confidentiality, integrity, and availability of CDPH PCI following an interruption or disaster event lasting more than twenty-four (24) hours.
- B. *CDPH PCI Backup Plan.*** Contractor shall have a documented, tested, accurate, and regularly scheduled full backup process for systems and devices holding CDPH PCI.

**V. Paper Document Controls**

- A. *Supervision of CDPH PCI.*** CDPH PCI in any physical format shall not be left unattended at any time. When not under the direct observation of an authorized Contractor workforce member, the CDPH PCI must be stored in a locked file cabinet, desk, or room. It also shall not be left unattended at any time in private vehicles or common carrier transportation, and it shall not be placed in checked baggage on common carrier transportation.
- B. *Escorting Visitors.*** Visitors who are not authorized to see CDPH PCI must be escorted by authorized workforce members when in areas where CDPH PCI is present, and CDPH PCI shall be kept out of sight of visitors.
- C. *Removal of CDPH PCI.*** CDPH PCI in any format must not be removed from the secure computing environment or secure physical storage of the Contractor, except with express written permission of the CDPH PCI owner.
- D. *Faxing and Printing.*** Contractor shall control access to information system output devices, such as printers and facsimile devices, to prevent unauthorized individuals from obtaining any output containing CDPH PCI. Fax numbers shall be verified with the intended recipient before transmittal.
- E. *Mailing.*** Mailings of CDPH PCI shall be sealed and secured from damage or inappropriate viewing to the extent possible. Mailings which include five hundred (500) or more individually identifiable records of CDPH PCI in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of CDPH to use another method is obtained.

## NOTICE OF INSURANCE COVERAGE

SAN BERNARDINO COUNTY  
 DEPARTMENT OF RISK MANAGEMENT  
**222 West Hospitality Lane, Third Floor**  
 San Bernardino, CA 92415-0016  
 (909) 386-8655 8-5 pm Mon-Fri  
 or after hours, call Communications Center at (909) 356-3805



San Bernardino County  
**DEPARTMENT OF RISK MANAGEMENT**  
 222 West Hospitality Lane, Third Floor  
 San Bernardino, CA 92415-0016

VICTOR TORDESILLAS  
 Director of Risk Management

### CERTIFICATE OF INSURANCE OR SELF-INSURANCE

In the event of cancellation of the self-insurance programs or policies designated below, it is the intent of the San Bernardino County to mail 30 days' prior notice thereof to:

#### TO WHOM IT MAY CONCERN

The San Bernardino County certifies that the following self-insurance programs or insurance policies are in force:

TYPE OF COVERAGE	COMPANY AND POLICY NO.	POLICY PERIOD	LIMITS OF LIABILITY	
			Bodily Injury	Property Damage
Comprehensive General Liability, Professional Liability incl. Auto Liability	Self-Insured	7/1/2023 through 7/1/2024	\$3,000,000 Combined Single Limits for Bodily Injury and Property Damage	
Workers' Compensation	Self-Insured	7/1/2023 through 7/1/2024	\$2,000,000	
Healthcare Professional Liability	Self-Insured	7/1/2023 through 7/1/2024	\$1,000,000 Combined Single Limits	

This Certificate is not valid unless countersigned by an authorized representative of the San Bernardino County, Department of Risk Management.

July 1, 2023

\_\_\_\_\_  
 Authorized Representative  
 Victor Tordesillas, Director