Center for Health Equity

UCSF

University of California
San Francisco

University of California, San Francisco
Center for Health Equity

Request for proposal

California Maternal Infant Health Assessment survey data collection 2025-2030

Date posted: August 12, 2024

Updated: August 19, 2024 (page 3)

Request for Proposal Overview

The Center for Health Equity at the University of California, San Francisco seeks a subcontractor for its contract with the California Department of Public Health to implement data collection for the Maternal and Infant Health Assessment. The proposed contract period is 5 years from April, 2025 – March, 2030 and will span data collections year 2025-2029. The proposed budget per year for the subcontractor is $825,000 - $950,000 per year.

RFP Contact

Monisha Shah
MIHA Project Manager
Email: monisha.shah@ucsf.edu

E-mail of intent to submit due date: September 10, 2024
Last date for questions: September 20, 2024
Proposal due date: September 27, 2024
Tentative award notification date: November 1, 2024
Contract term: April 1, 2025 – March 30, 2030.

Incomplete proposals or those received after the due date will not be evaluated.

Table of Contents

Appendices

Overview

University of California, San Francisco, Center for Health Equity

The University of California, San Francisco (UCSF) Center for Health Equity (CHE) plays a leading role in research looking at upstream factors to improve health equity in the United States. Improving health equity entails removing obstacles to health such as poverty, discrimination, racism, powerlessness, and the consequences of those obstacles. One of CHE's strengths is survey research, including design, implementation, analyses, and dissemination of findings. The UCSF CHE Maternal and Infant Health Assessment team focuses its efforts on health equity among birthing people and their infants.

Maternal and Infant Health Assessment

The Maternal and Infant Health Assessment (MIHA) is a population-based survey of women with a recent live birth in California, conducted annually since 1999. MIHA collects self-reported information about maternal and infant experiences and about maternal attitudes and behaviors before, during and shortly after pregnancy. MIHA results are used to improve our understanding of the health of people having babies (hereafter described as birthing people) and infants across California to inform public health programs and clinical practice, and assist program planners in prioritizing limited resources.

MIHA is led by the Maternal, Child and Adolescent Health (MCAH) Division in collaboration with the Women, Infant & Children (WIC) Division of the California Department of Public Health and UCSF CHE. The MIHA survey has been partially supported by the California Department of Public Health using federal funds from the Title V Maternal and Child Health Block Grant and the Special Supplemental Nutrition Program for Women, Infants and Children.

MIHA sample and data collection overview

Each year, UCSF randomly samples approximately 10,000 individuals with a recent live birth from California birth certificates in four monthly batches of about 2,500 birthing people each (typically, February-May). The sample includes an oversample of high-priority populations, currently Black birthing people and those with a preterm birth, to ensure that their adequate representation in the study. The sample is stratified by county of residence to facilitate local estimates for 36 California counties.

MIHA data are collected using three modes: self-administered paper questionnaires delivered by mail (SAQ), web questionnaires, and CATI. UCSF may make changes to data collection methods at any point, though changes during the annual data collection period are rare. The MIHA questionnaire is revised annually and includes core questions, questions that cycle, and short-term questions to address evolving public health priorities. Sampled individuals are first contacted via mail, with an option to complete the survey by phone or web. Non-respondents are subsequently contacted by telephone, text, and/or email until 11 months postpartum, when the sampled person is no longer eligible to participate. Sampled individuals receive a cash incentive, are offered a gift card for completing the survey, and are invited to participate in a raffle. MIHA is currently conducted in English and Spanish; approximately 82% of the responses are completed in English and 18% in Spanish. In future years, UCSF may offer MIHA in additional languages. MIHA has obtained a response rate of around 54-60% for the past 4 years.

Summary of scope for MIHA 2025 - 2030

General overview

The subcontractor shall be responsible for implementing MIHA survey data collection activities in English and Spanish per the MIHA protocol approved by the California Health and Human Services Committee for the Protection of Human Subjects (CPHS) with a 55% response rate. Subcontractor data collection responsibilities include:

- Conducting staff training and ensuring staff competency;
- Supporting UCSF annual questionnaire pretesting and finalization;
- Development of a cost-effective and efficient software solution for MIHA survey sample management and tracking of data collection activities, annual programming of CATI and web survey platforms, implementation of CATI and web survey data collection, data entry of self-administered questionnaires, data management of survey data from all modes, reporting, and data file output;
- Development of a data collection timeline;
- Respondent tracing, including obtaining email and phone contact information;
- Printing and mailing of the self-administered questionnaire and related materials, including management of cash incentives;
- Receipt, management, data entry, and temporary storage of completed self-administered questionnaires in English and Spanish, including contact information tear sheets from the end of the survey, and procurement and provision of gift card rewards to respondents;
- Implementation of CATI operations in English and Spanish;
- Implementation of web survey operations in English and Spanish;
- Delivery of data sets to UCSF, including one preliminary and one final single dataset of survey responses from all three modes, an operations dataset, a comments/open-ends dataset, and a follow-up contact information data set; and
- Participation in meetings and site visits with UCSF.

Specific subcontractor tasks and details are described below.

Staff training and competency –Updated 8/19/2024

Human subjects research training

The subcontractor shall ensure that all staff and external partners (e.g., printer) working on MIHA or who have contact with study participant information complete CITI human subjects research training. Training shall be updated when expired. The subcontractor shall provide UCSF with certificates of training prior to the start of data collection, or prior to contact with study participant information, for new staff.

Interviewer competency and training

The subcontractor will retain professional interviewers who are experienced in conducting interviews with people on sensitive topics such as reproductive or maternal health and who demonstrate a high

level of skill in telephone interview best practices, particularly building rapport and maintaining neutrality. We prefer that interviewers not be short-term, temporary, or student workers. The subcontractor should ensure adequate staffing of interviewers whose native language is Spanish (Mexican and Central American dialects). To date, just over half of the phone interviews have been in English and the rest in Spanish. The subcontractor should also retain interviewers who are concordant with racial or ethnic groups oversampled in MIHA (currently, Black birthing people).

The subcontractor shall be responsible for training new and current interviewers and supervisors on telephone interviewing techniques and best practices, and for ensuring that all interviewers and supervisors are trained on annual MIHA questionnaire changes and the *MIHA Telephone Interviewer Guide* (see CATI data collection). UCSF will participate in trainings on annual questionnaire changes.

Questionnaire pretesting and finalization

UCSF revises questionnaire content annually. UCSF conducts annual pretesting in English and Spanish of new questions and question revisions, using a variety of methods, including a web pretest survey (developed and implemented by UCSF), virtual or in-person focus groups, cognitive interviews, and field tests. The subcontractor shall provide support to questionnaire development and pretesting activities, which will include review of (a) any new questions to identify possible difficulties in survey administration in all modes, (b) Spanish translations, and (c) final SAQ questionnaire for typos and other errors; and recruitment of California resident birthing people for English and Spanish pretesting. Additional testing of programmed web survey and CATI instruments are described in "Questionnaire data collection software programming."

UCSF will deliver the annual questionnaire content in MS Word to the subcontractor, including the formatted self-administered paper (SAQ), telephone (TAQ), and web (WAQ) versions of the questionnaire.

Data management

The subcontractor shall develop and implement a cost-effective and efficient software solution for MIHA survey data collection, including sample tracking and management, implementation of CATI and web survey data collection, SAQ data entry, editing and management of survey data from all modes, and reporting and data file output. The subcontractor shall complete the UCSF IT Security Office review of the data collection and sample management software platform(s) and receive approval prior to implementation of data collection. The subcontractor shall complete UCSF IT Security Office review of any new software that will manage personal and confidential information, as defined by CDPH in Appendix B, for individuals in the MIHA sample prior to implementation.

MIHA data are owned by the California Department of Public Health. UCSF manages all final data and conducts analyses of study results. No analyses of study results are needed by the contractor.

Tracking and operations database

UCSF monitors MIHA operational practices, conducts analyses of operations data, and implements operational experiments in order to understand and improve data collection practices and survey response. The subcontractor shall develop and maintain a tracking database that documents all data

collection activities and the disposition of each activity for each sampled individual and documents the current status of each sampled individual throughout data collection with minimum content specified by UCSF.

Tear sheet database

The subcontractor shall establish a database or file and enter follow up contact information and responses included on the survey tear sheet that shall be kept separate from other survey response information.

Questionnaire data collection software programming

The subcontractor shall use the SAQ, TAQ, and WAQ Word documents provided by UCSF to program the SAQ data entry database and CATI and web survey platform(s) and update each instrument with annual questionnaire revisions. The subcontractor shall work with UCSF to develop a *Master Editor* document that includes guidelines for out-of-range values and survey logic errors, editing instructions, and data entry procedures.

The subcontractor shall test the full CATI instrument in English and Spanish with at least four live participants in each language. The subcontractor shall provide UCSF with a mechanism to both listen in and observe CATI screens and data entry for all test interviews either through real-time observation or recorded interviews. The subcontractor shall recruit participants according to specified characteristics for CATI pretesting. The subcontractor will test CATI survey logic and provide UCSF with a mechanism for reviewing the CATI survey logic programming and interviewer instructions and probes. As needed, the subcontractor shall implement CATI edits as specified by UCSF and conduct additional tests with live respondents. The subcontractor shall enable UCSF to review revisions to CATI programming.

The subcontractor shall test the web survey in English and Spanish for accuracy of content and survey logic and skip patterns. The subcontractor shall allow UCSF to review and test the respondent view of the web survey and provide a mechanism for reviewing survey logic programming. The subcontractor shall implement web survey edits as specified by UCSF and enable UCSF to review revisions to web survey programming.

Data collection timeline

Prior to the start of data collection, the subcontractor shall work with UCSF to develop a joint data collection timeline that identifies all planned data collection tasks by batch, entity responsible, and due date.

Contact information and tracing

Prior to the start of data collection for each batch, UCSF will provide the sample of births to the subcontractor in a dataset that includes identifying information, street and mailing addresses, and individual characteristics, including whether the sampled individual is a likely Spanish-speaker. Prior to the start of CATI operations for each batch, UCSF will provide to the subcontractor phone numbers for approximately 80% of sampled individuals. New contact information will be provided by UCSF to the

subcontractor later in data collection. The subcontractor shall upload and merge sample and contact data files into their tracking database.

The subcontractor shall develop and implement innovative and efficient approaches to obtain additional mail, telephone, and email information for sampled individuals via other methods, in accordance with the Human Subjects Research protocol and with UCSF approval.

Self-administered questionnaire data collection

Printing and Mailing

The subcontractor shall be responsible for implementing printing and mailing activities, including proof development; procurement of paper, envelopes, postage, cash incentives, and other inserts (e.g., flat pens provided by UCSF); envelope and packet assembly; and postage affixation. UCSF may revise these materials from year to year. Each year, UCSF will provide to the subcontractor formatted electronic MS Word files of all printed and mailed material, including text content for postcards and envelopes. The subcontractor will create and provide to UCSF for approval proofs of printed versions of the questionnaire and all other mailed material, in all languages, prior to printing.

The subcontractor will assemble all mailings and mail them according to the data collection timeline. The subcontractor will develop a process for procuring and tracking cash incentives included in the first mailing of each batch. See Appendix A for a list of mailings, materials specifications, and estimated quantities. UCSF Documents and Media has conducted the proofing, printing, packet assembly, and mailing since 2010. The subcontractor may continue contracting with UCSF Documents and Media or use an alternative approach. The subcontractor shall conduct re-mails of the questionnaire on an as-needed basis.

Return mail

Assume a 25% response rate by mail (~2,500), and another 7% returned postcards (~700). The subcontractor shall log each piece of returned mail (undeliverable or a completed survey) in the tracking database at least twice per week.

Rewards

The subcontractor shall send MIHA respondents thank-you letters written by UCSF and a Target or Amazon gift card for participation in amounts that increase as data collection progresses (UCSF has been offering $15, increasing to $20, $30, and $40). The subcontractor shall purchase, distribute, and track gift cards according to a plan developed in collaboration with UCSF. Thank-you letters do not need to be personalized.

Mail questionnaire data entry

The subcontractor shall develop a process to enter data efficiently and accurately from completed SAQs in accordance with the MIHA protocol. The subcontractor shall implement validation practices to ensure accuracy of the SAQ data entry. UCSF shall have the opportunity to approve the editing and validation procedures or tests.

CATI data collection

Phone interviews using the CATI system begin about two months into data collection with non-respondents. Assume that 75% of nonrespondents will be sent to telephone interviewing (1,800 – 2,000 during each batch). Approximately half of phone interviews are conducted in Spanish.

Interviewer staffing

The subcontractor will assign enough interviewers to MIHA to ensure the data collection timeline is followed, productivity targets are met, and progress toward response rates is maintained. The subcontractor shall schedule MIHA CATI interviewing during morning through evening hours on weekdays and weekends.

CATI operations

The subcontractor shall advise UCSF on CATI operations that will improve cost-efficiency and maintain or improve CATI response rates and document standardized CATI operations in the *MIHA Telephone Interviewer Guide* for UCSF approval. The subcontractor shall conduct telephone outreach and telephone interviews via CATI in English and Spanish, including conversion of soft refusals, according to the MIHA protocol, the *MIHA Telephone Interviewer Guide,* and federal laws to achieve the target response rate. The results of each call shall be tracked and include variables specified by UCSF. The subcontractor shall implement CATI operations onsite. Remote CATI operations may be implemented in contingency scenarios (e.g., power outage, public health emergency) with approval of UCSF using protocols that conform to human subjects and data privacy requirements.

CATI quality assurance and monitoring

The subcontractor shall implement procedures for assuring and documenting the quality of the telephone interview process and the entry of survey responses and verbatim documentation of open-ended responses into CATI software. Quality activities shall include regular monitoring of all interviewers in both English and Spanish to ensure adherence to the MIHA protocol, protection of respondent confidentiality during respondent identification and interviewing, and physical security of materials at interview stations. Quality assurance reports shall be provided to UCSF via e-mail on a monthly basis or verbally during the bi-weekly meetings. The subcontractor shall make remote monitoring available to allow UCSF to hear both the interviewer and respondent during initial contact, consent, and interview process and observe data entry for periodic quality assurance.

Web survey

Sampled individuals are offered the opportunity to complete the survey on the web in the first mailing, reminder post card, during telephone contacts, and by text or email. The subcontractor shall advise on web survey methods based on industry best practices to improve overall MIHA response rate and cost effectiveness.

MIHA survey website

The subcontractor shall host and maintain the MIHA web survey and a MIHA survey domain website that provides information about the survey for sampled individuals with links to the web survey, the MIHA resources list, and CDPH MIHA website according to specifications provided by UCSF.

Text and email outreach

The subcontractor shall develop and implement a strategy for text outreach and delivery of the web survey link and study ID number to promote survey response, with UCSF approval. UCSF will provide text scripts, which the subcontractor can modify with UCSF approval. The strategy shall describe timing and sequence of contacts and specific texting practices and shall follow federal law and MIHA protocol in texting practices. Expect to text approximately 6,300 individuals.

The subcontractor shall establish a project-specific email address. The subcontractor shall develop and implement a strategy for email outreach and delivery of the web survey link to promote survey response, with UCSF approval. The strategy should include development of an engaging MIHA email template, timing and sequence of contacts, and specific email practices. UCSF will provide email scripts, which the subcontractor can modify with UCSF approval. Expect to email approximately 3,000 individuals.

MIHA datasets

Operations datasets

The subcontractor shall produce an annual operations dataset. The subcontractor shall collaborate with UCSF to identify and define standard operational dataset variables that will be used by UCSF to conduct analyses and comparisons with prior years. The subcontractor shall deliver to UCSF the final operational dataset in a mutually agreed upon format and an associated codebook by the end of March each year.

MIHA survey datasets

The subcontractor shall deliver to UCSF via secure transmission a single, concatenated, SAS-accessible preliminary data set, including data collected through September from the SAQ, web survey, and CATI, by the beginning of November each year. The subcontractor shall deliver to UCSF via secure transmission a single, concatenated, SAS-accessible file of final survey data from the paper questionnaire, web survey, and CATI by the end of March each year.

The subcontractor shall provide a file containing all verbatim write-in data from open-ended responses and end-of-survey prompt linked to survey ID numbers, with names redacted (if present). The comments shall not be truncated due to length. Survey question open-ended responses shall be delivered by the end of March each year. The due date of the end-of-survey prompt is negotiable.

Follow-up contact information dataset

The subcontractor shall deliver to UCSF via secure transmission a data file of tear sheet data March.

Data security

All sample data are considered personal and confidential information, as defined by CDPH in Appendix B. Sample data are derived from California Vital Records data and thus must follow the Information Privacy and Security Requirements (IPSR) from California Department of Public Health (CDPH), Center for Health Statistics and Informatics (CHSI) Vital Statistics Advisory Committee (VSAC), including but not limited to physical protections, back-up procedures, and file transmission. The IPSR can be found in Appendix B.

Physical surveys

During data collection, the subcontractor shall maintain completed physical surveys according to data security guidelines during and after data entry. After surveys have been data entered, the tear sheets with follow up contact information shall be removed from the survey and kept in a separate location from the questionnaire booklets. After all data entry is complete, the subcontractor shall collaborate with UCSF and CDPH to securely transfer physical surveys to a State storage facility according to CDPH requirements. The tear sheets shall be shredded or transferred separately to State storage, as specified by CDPH.

Progress monitoring by UCSF

Meetings and site visits

The subcontractor shall participate in virtual meetings with UCSF including: 1) a kick-off meeting to review the project scope and start-up workplan; 2) bi-weekly meetings to discuss MIHA data collection planning, programming, and questionnaire pretesting; 3) an annual interviewer debrief meeting shortly after the completion of data collection; and 4) an annual operational meeting, generally in April, to discuss operational challenges in data collection and plans for the next annual data collection cycle.

The subcontractor shall accommodate at least one annual site visit from UCSF.

Data collection progress reports

The subcontractor shall provide to UCSF weekly overall response rate reports during data collection, and bi-monthly progress reports that present response rates by sampling characteristics and historical comparisons (if available), as specified by UCSF. The subcontractor shall provide individual response status by identification number upon UCSF request.

Additional scope of work

UCSF may undertake additional studies in future years, such as an enhancement of MIHA data collection practices for specific populations of birthing people or follow-up studies of MIHA respondents.

UCSF may pilot a one-year Asian American, Native Hawaiian, and Pacific Islander (AANHPI) MIHA enhancement, which would include an expanded sample of an additional 1,000 AANHPI birthing people, implementation of the survey in additional languages in all modes, and adapted study materials, such as revised mailed questionnaire package inserts for specific AANHPI subgroups. If UCSF implements the pilot for one year, the subcontractor shall conduct data collection activities for an additional 1,000 sampled individuals (approximately 250 per batch) and implement mailed survey data entry, CATI, and web survey operations in three additional written and spoken languages. MIHA already samples AANHPI individuals. The total AANHPI sample will likely be about 1,800-2,100 with the enhancement. Assume written languages are Chinese simplified, Chinese traditional, and Vietnamese. Assume spoken languages are Mandarin, Cantonese, and Vietnamese. The subcontractor shall ensure that printing and mailing operations account for increased sample size and increased complexity of preparing unique packets for additional AANHPI subgroups.

Proposal Submission Requirements

This section contains instructions for Bidders to use in preparing their proposals. Please use the instructions laid out below to demonstrate the Bidder's experience and ability to perform the requirements specified throughout this document.

Proposal format

1. Provide a cover page with the following elements:
    a. Organization Name
    b. Chief executive name and title
    c. Telephone, email, address
    d. Lead point of contact if different than above
    e. Point of contact telephone, email, address, if different than above.
2. Provide one electronic copy of the proposal labelled with the Bidder's name.
3. Number all pages of the proposal, including forms and attachments, and include the Bidder's name in the header.
4. All electronic documents should be formatted for printing, including the budget documents.
5. It is the responsibility of the Bidder to provide all information requested in this RFP package at the time of submission.

Proposal Contents

Please submit the following information:

Section I. Organization Qualifications and Experience

Provide a description of no more than 10 pages specifying the information outlined below.

1. Overview of the organization

Describe the organization's qualifications, skills, and capacity to provide the requested services in this RFP. Include three examples of projects, within the past five-seven years, that demonstrate experience and expertise performing these services and highlighting the Bidder's qualifications, skills, and capacity. For each project, provide the sample size and response rates, specify the modes of data collection, and list the project period. At minimum, address organizational qualifications and experience in (a) identification and application of software solutions for multi-mode surveys; (b) sample management for multi-mode surveys; (c) implementation of mailed paper surveys, web surveys, and CATI operations in English and Spanish; (d) data management; and (e) contact tracing.

2. Organizational chart

Provide an organizational chart of the Bidder's organization, identifying staff/positions assigned to the project, corresponding job titles. Describe how subcontractors and consultants, if any, will interact with the Bidder's organization (i.e., oversight and management of the subcontractor). Please identify remote staff and explain supervision.

3. Staff credentials

Include brief descriptions of key staff credentials or experience relevant to this scope of work. Include resume or CV for each.

4. Quality control, corrective action, and data privacy

Provide descriptions of systems that will be used to maintain quality control, including for remote workers. Describe corrective measures the Bidder will take to improve contact tracing and response rate, quality of interviews, and data entry. Describe organizational policies and practices for protecting data privacy that conform to the requirements set forward in the CDPH Information Privacy and Security Requirements (Appendix B). Describe policies and practices for addressing data breaches.

5. Contingency plan scenarios

Describe contingency plans to continue normal operations described in this RFP in the case of an unexpected event or situation, such as power outage, severe weather, or pandemic. Describe plans and policies specific to both onsite operations and remote workers.

6. References

The bidder should provide the organization name and contact information for three references that can attest to the organization's qualifications and experience in providing services similar to the requested services in this RFP.

7. Subcontractors or consultants

If subcontractors or consultants are to be used, for example, for printing and mailing operations, provide a list that specifies the name, address, phone number, email, contact person, and a brief description of the Bidder's subcontractor's organizational capacity and specific qualifications.

Section II. Proposed services

1. Services to be provided

Provide a narrative description of no more than 20 pages specifying the services and approach the Bidder will offer to address the Scope of Services of this RFP.

In addition to other information you feel is relevant, please address these specific elements in the services narrative:

- Provide one *preferred* software option for implementing sample tracking, survey implementation, and survey data management requirements specified in this RFP and one *alternative* option. For each option, describe what software will be used for sample tracking/management, data entry, web survey, and CATI; describe how the software solution for each mode and function will be integrated, if at all. For each option, describe the pros, cons, and limitations.
- Describe strategy for implementing start-up activities to ensure quality, accuracy, and timeline of data collection components described in the scope of work are maintained.
- Describe strategies and mechanisms proposed for contact tracing and sample management, including obtaining emails and phone numbers.

- Describe plan for SAQ printing and mailing processes, including plan to ensure data collection timeline is maintained.
- Describe mechanisms for procuring, managing, and providing cash incentives and gift card rewards.
- Describe procedures for annual CATI and web programming, including for assuring accuracy of content and survey logic, and for facilitating UCSF reviews.
- Describe procedures for data entry and quality checking.
- Describe existing interviewer staffing capacity and qualifications, languages spoken, and how new interviewers would be brought on for this project.

- Describe planned format and procedures for sharing final survey and operational data sets.

2. Implementation work plan

Provide a workplan in the form of a timeline chart for the implementation of MIHA data collection from the initial implementation of this contract in April 2025 through March 2026 when MIHA datasets are provided to UCSF. Concisely describe each program development and implementation task, the month it will be carried out, and the person or position responsible for each task. Note tasks that would be delegated to subcontractors or consultants, if any. Demonstrate an approach to project start up or development tasks that accounts for iterative review, adaptation, and approval of individual project components.

Section III. Cost proposal

For the first year of this contract term, provide an itemized cost proposal and justification that includes all aspects of providing the scope of services described in this RFP. For years 2-5, provide only the total budget. The itemized budget should include line items within the following minimum categories: (a) staff salary and benefits, (b) operating expenses, (c) printing and mailing, (d) incentives and rewards, and (e) indirect costs, if any. If subcontractors will be used for any scope of work activities, specify and provide the estimated cost of the subcontract in the itemized budget. The budget justification should include a detailed description of each budget line item and an explanation of how the costs proposed will fulfill the requirements specified in the scope of this RFP. Indicate one-time costs or substantial cost differences expected between year 1 and subsequent years. The cost proposal for each year of this proposal shall not to exceed the $825,000 - $950,000 annual range. Do not include the cost of the additional scope of work (see below) in this cost proposal.

The following details may assist the Bidders in the development of the cost proposal:

- The current budget for UCSF Documents and Media is estimated at $155,000-$170,000/year. See Appendix A for details about mailing requirements.
- Assume a 25% response rate by mail (~2,500), and another 7% returned postcards (~700).
- Assume a yearly cash incentives and gift card budget of about $155,000 total.
- Assume an annual transfer of 10-20 boxes of physical surveys to State storage.

Section IV. Additional scope of work for AANHPI MIHA Enhancement

1. Services to be provided

Provide a separate two-page description of organization qualifications, experience and services to be provided for the implementation of the additional scope of work for the AANHPI MIHA Enhancement. The qualifications and experience and services should specify capacity and plan to implement data collection, including programming of instruments, interviewing, data editing and entry, and to field inquiries from sampled individuals in the languages identified in the additional scope of work section of this RFP. Explain quality assurance and supervision for data collection activities conducted in AANHPI languages. Specify any additional AANHPI language capacity of the Bidder beyond the AANHPI languages specified.

2. Cost proposal

Provide the total cost estimate for the additional scope of work for the AANHPI MIHA Enhancement with the description. The cost proposal for the additional scope of work is not to exceed the $75,000-$100,000 range.

Evaluation criteria

Qualified reviewers will judge the merits of the proposals received in accordance with the criteria defined in this RFP.

Proposal scoring

The overall score will be based on a 100-point scale:

- Organization qualifications and experience, including references (25 points)
- Services narrative (25 points)
- Implementation workplan (15 points)
- Cost proposal (25 points)
- Additional scope of work (10 points)

Finalist interviews

Based on final scores, up to three finalists will be selected to participate in in-person or virtual interviews.

Requirements prior to contract execution

Prior to contract execution, the awarded Bidder may be required to submit additional materials, included but not limited to Certificate of Insurance. UCSF reserves the right to negotiate the final scope of work and costs with the awarded Bidder. Some costs and activities are negotiable, and may depend on the Bidder's expertise and contacts. If an acceptable contract cannot be negotiated with the awarded bidder, UCSF may withdraw its offer and negotiate with the next bidder.

Appendix A

Printing specifications

Provide an estimate of all printed and mailed materials as described below.

Advance letter
Mailed 3 ½ weeks after sampling to all sampled individuals, approximately 10,000.

Item	Description
Envelope	Envelope addressed to sampled individual with contractor's return address in upper corner. #10 envelopes: 4 1/8 x 9 1/2, 24# white wove,, black ink Manually affixed postage.
Advance Letter	Letter in English on one side and Spanish on other side. Color: White paper, black and white text 20# Bond white 8 ½ x 11, black ink 2-s, head to foot
Postcard – address update	Postage-paid postcard to send back with updated address. In English for likely English speakers and in Spanish for likely Spanish speakers. English-67# Exact Vellum Bristol Yellow; Spanish-67# Exact Vellum Bristol Orange 5 ½ x 3 ¾ , black ink 2-s

First questionnaire
Mailed 1 ½ weeks after Advance to all sampled individuals with an address, approximately 10,000.

Item	**Description**
Questionnaire	Body – 60# offset white, black ink throughout with no bleed; cover- black + 1 PMS one side with full bleeds, 80# dull coated cover white, saddle stitch, final size 8.5x11; PMS 285 blue for English and 7670 purple for Spanish
Envelope	Addressed to sampled individual with contractor's return address in upper corner. Affixed postage. 28# manila catalog envelope, black ink
Cover letter	Contains all elements of informed consent in English on one side and Spanish on other side. 20# Bond white 8 ½ x 11 , black ink 2-s, head to head
Insert	Small bright paper describing raffle opportunity and reminder of gift card for participating

	60# Astrobright Gemini Green 8.5 x 3.667, black ink 2-s
Postcard – Spanish	Postage-paid postcard to request other language Spanish-67# Exact Vellum Bristol Orange 5 ½ x 3 ¾ , ink 2-s
Postcard – English	Postage-paid postcard to request other language English-67# Exact Vellum Bristol Yellow; black ink 2-s
Return envelope	Postage paid (BRM account) and contractor's return address. 28# white catalog envelope, black ink
Pen	Flat pen provided by UCSF with MIHA tagline
Incentive	$5 bill for African American $1 bill for others

Reminder postcard
Mailed 2 weeks after first packet, to all non-respondents, approximately 8,850.

Item	**Description**
Postcard	Postcard reminding individuals to complete the survey. 100# Matte cover 8 ½ x 5 ½, 4 cp/black w/ bleeds

Second questionnaire
Mailed 1 ½ - 2 weeks after reminder postcard to all non-respondents, approximately 7,850.

Item	**Description**
Questionnaire	Body – 60# offset white, black ink throughout with no bleed; cover- black + 1 PMS one side with full bleeds, 80# dull coated cover white, saddle stitch, final size 8.5x11; PMS 285 blue for English and 7670 purple for Spanish
Envelope	Addressed to sampled individual with contractor's return address in upper corner. Affixed postage. 28# manila catalog envelope, black ink
Cover letter	Contains all elements of informed consent in English on one side and Spanish on other side. 20# Bond white 8 ½ x 11 , black ink 2-s, head to head
Insert	Small bright paper describing raffle opportunity and reminder of gift

	card for participating 60# Astrobright Gemini Green 8.5 x 3.667, black ink 2-s
Postcard – Spanish	Postage-paid postcard to request other language Spanish-67# Exact Vellum Bristol Orange 5 ½ x 3 ¾ , ink 2-s
Postcard – English	Postage-paid postcard to request other language English-67# Exact Vellum Bristol Yellow; black ink 2-s
Return envelope	Postage paid (BRM account) and contractor's return address. 28# white catalog envelope, black ink

Fall/Holiday Postcard
Mailed to non-respondents in fall or around winter holidays, depending on batch and response rate, approximately 5150.

Fall/ Holiday Postcard	Postcard for selected non-responders (TBD during data collection), offering a $40 gift card to complete the survey. Includes link to web survey.

Thank you letter and gift card
Mailed after survey is completed, approximately 5,500.

Envelope	Addressed to respondent with contractor's return address in upper corner. Postage. 4 1/8 x 9 1/2, 24# white wove #10 envelope, black ink
Thank you letter	Letter in English on one side and Spanish on other side. 20# Bond white 8 ½ x 11, black ink 2-s, head to foot

California Department of Public Health
Center for Health Statistics and Informatics

Data Application
Agreement
Information Privacy and Security Requirements

This Information Privacy and Security Requirements Exhibit (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 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 7920.530, or is exempt from disclosure under any of the provisions of Section 7920.000, 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.

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

California Department of Public Health
Center for Health Statistics and Informatics

Data Application
Agreement
Information Privacy and Security Requirements

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, or analysis of information.

California Department of Public Health
Center for Health Statistics and Informatics

Data Application
Agreement
Information Privacy and Security Requirements

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 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 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.

California Department of Public Health
Center for Health Statistics and Informatics

Data Application
Agreement
Information Privacy and Security Requirements

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

California Department of Public Health
Center for Health Statistics and Informatics

Data Application
Agreement
Information Privacy and Security Requirements

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.

California Department of Public Health
Center for Health Statistics and Informatics

Data Application
Agreement
Information Privacy and Security Requirements

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 c/o Office of Legal Services California Dept. of Public Health P.O. Box 997377, MS 0506 Sacramento, CA 95899-7377 Email: privacy@cdph.ca.gov Telephone: (877) 421-9634	Chief Information Security Officer Information Security Office California Dept. of Public Health P.O. Box 997413, MS 6302 Sacramento, CA 95899-7413 Email: CDPH.InfoSecurityOffice@cdph.ca.gov Telephone: (855) 500-0016

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 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.

XIV. 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.

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 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.

California Department of Public Health
Center for Health Statistics and Informatics

Data Application
Agreement
Information Privacy and Security Requirements

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.

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 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 and XI of this Exhibit shall survive the completion or termination of the agreement between Contractor and CDPH.

California Department of Public Health
Center for Health Statistics and Informatics

Data Application
Agreement
Information Privacy and Security Requirements

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 its 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 and mobile computing devices must be encrypted, in accordance with CDPH Cryptographic Standards or using the latest FIPS 140 validated cryptographic modules.

- All electronic files that contain CDPH PCI must be encrypted when stored on any removable media type device (such as USB thumb drives, CD/DVD, tape backup, etc.), in accordance with CDPH Cryptographic Standards or using the latest FIPS 140 validated cryptographic modules.

- CDPH PCI must be encrypted during data in-transit and at-rest on all public telecommunications and network systems, and at all points not in the direct ownership and control of the Department, in accordance with CDPH Cryptographic Standards or using the latest FIPS 140 validated cryptographic modules.

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.

California Department of Public Health
Center for Health Statistics and Informatics

Data Application
Agreement
Information Privacy and Security Requirements

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 action 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 publication or availability of 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. To access systems/applications that store, process, or transmit CDPH PCI, it must comply with SIMM 5360-C Multi-factor Authentication (MFA) Standard and NIST SP800-63B Digital Identity Guidelines. The SIMM 5350-C provides steps for determining the Authenticator Assurance Level (AAL), and a set of permitted authenticator types for each AAL (0-3). Note: MFA requirement does not apply to AAL 0.

All Contractor workforce members are required to leverage FIDO authentication. The FIDO authentication is AAL 3 compliance. FIDO certified devices such as YubiKeys and Windows Hello for Business (WHfB) are the mechanism for user authentication in the Department.

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.

	AAL 1	AAL 2	AAL 3
Permitted Authenticator Types	- Memorized Secret - Look-Up Secret - Out-of-Band Devices - Single-Factor One-Time Password (OTP) Device - Multi-Factor OTP Device - Single-Factor Cryptographic Software - Single-Factor Cryptographic Device - Multi-Factor Cryptographic Software - Multi-Factor Cryptographic Device	- Multi-Factor OTP Device - Multi-Factor Cryptographic Software - Multi-Factor Cryptographic Device - Memorized Secret **plus**: - Look-Up Secret - Out-of-Band Device - Single-Factor OTP Device - Single-Factor Cryptographic Software - Single-Factor Cryptographic Device	- Multi-Factor Cryptographic Device - Single-Factor Cryptographic Device used in conjunction with Memorized Secret - Multi-Factor OTP device (software or hardware) used in conjunction with a Single-Factor Cryptographic Device - Multi-Factor OTP device (hardware only) used in conjunction with a Single-Factor Cryptographic Software - Single-Factor OTP device (hardware only) used in conjunction with a Multi-Factor Cryptographic Software Authenticator - Single-Factor OTP device (hardware only) used in conjunction with a Single-Factor Cryptographic Software Authenticator and a Memorized Secret.

California Department of Public Health
Center for Health Statistics and Informatics

Data Application
Agreement
Information Privacy and Security Requirements

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. ***Reauthentication.*** Contractor's computing devices holding, or processing CDPH PCI must comply the Reauthentication requirement, in which a session must be terminated (e.g., logged out) when the specified time is reached. Note: Reauthentication requirement does not apply to Authenticator Assurance Level (AAL) 0.

	AAL 1	**AAL 2**	**AAL 3**
Reauthentication	30 Days – Fix Period of Time, regardless user activity	12 hours – Fix Period of Time, regardless user activity; 30 minutes inactivity May use one of the authenticators to reauthenticate	12 hours – Fix Period of Time regardless user activity; 15 minutes inactivity Must use both authenticators to reauthenticate

In addition, reauthentication of individuals is required in the following situations:

- When authenticators change
- When roles change
- When the execution of privileged function occurs (e.g., performing a critical transaction)

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 its 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 six (6) years after event occurrence. There must protect audit information and audit logging tools from unauthorized access, modification, and deletion. There must also be a documented and routine procedure in place to review system logs for unauthorized access.

K. Live Data Usage. Using live data (production data) for testing and training purposes is not allowed. Synthetic data must be used. If synthetic data cannot be generated and/or used, a de-identification process against the live data must be done to reduce privacy risks to individuals. The de-identification process removes identifying information from a dataset so that individual data cannot be linked with specific individuals. Refer to CHHS Data De-Identification Guidelines.

L. Privileged Access Management (PAM). Contractor who responsible for setting up and maintaining privileged accounts related to CDPH electronic information resources shall comply with the CDPH PAM Security Standard. Information resources include user workstations as well as servers, databases, applications, and systems managed on-premises and on the cloud.

California Department of Public Health
Center for Health Statistics and Informatics

Data Application
Agreement
Information Privacy and Security Requirements

M. 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 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.

California Department of Public Health
Center for Health Statistics and Informatics

Data Application
Agreement
Information Privacy and Security Requirements

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.

I, the undersigned, on behalf of the agency represented in this application, and under penalty of perjury under the laws of the State of California, accept all terms, provisions, and conditions of this application.

Applicant Name *(If the person signing this form is other than the principal investigator or co-principal investigator, please indicate your authority to sign on the organization's behalf):*					
Name of Organization:					
Organization Address *(physical location where vital records data will be stored and accessed)**:***					
City:		**State:**		**Zip:**	
Applicant Signature:		**Date:**			