

STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES

STANDARD AGREEMENT

STD 213 (Rev. 03/2019)

AGREEMENT NUMBER

21-30049-000

PURCHASING AUTHORITY NUMBER (If Applicable)

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

CONTRACTING AGENCY NAME

Department of State Hospitals - Patton

CONTRACTOR NAME

County of San Bernardino on behalf Arrowhead Regional Medical Center

2. The term of this Agreement is:

START DATE

August 14, 2021 or upon DSH approval

THROUGH END DATE

August 13, 2024

3. The maximum amount of this Agreement is:

\$0.00, Zero Dollars and Zero Cents

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

Exhibits	Title	Pages
Exhibit A	Scope of Work	3
Exhibit A-1	Student Privacy Acknowledgement and Nondisclosure Agreement	1
Exhibit A-2	Student and Instructor Requirements and Responsibilities	3
+ - Exhibit B	Budget Detail and Payment Provisions	1
+ - Exhibit C *	General Terms and Conditions	N/A
+ - Exhibit D	Special Terms and Conditions Interagency Agreement	3
+ - Exhibit E	Confidentiality and Information Security Provisions (HIPAA Business Associate Agreement)	1
+ - Exhibit F	Information Privacy and Security Requirements (Non-HIPAA/HITECH Act Contracts)	10

Items shown with an asterisk (*), are hereby incorporated by reference and made part of this agreement as if attached hereto.

These documents can be viewed at <https://www.dgs.ca.gov/OLS/Resources>

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.)

County of San Bernardino on behalf Arrowhead Regional Medical Center

CONTRACTOR BUSINESS ADDRESS

400 N. Pepper Avenue

CITY

Colton

STATE

CA

ZIP

92324

PRINTED NAME OF PERSON SIGNING

Curt Hagman

TITLE

Chairman, Board of Supervisors

CONTRACTOR AUTHORIZED SIGNATURE

DATE SIGNED

STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES

STANDARD AGREEMENT

STD 213 (Rev. 03/2019)

AGREEMENT NUMBER

21-30049-000

PURCHASING AUTHORITY NUMBER (If Applicable)

STATE OF CALIFORNIA

CONTRACTING AGENCY NAME

Department of State Hospitals - Patton

CONTRACTING AGENCY ADDRESS

3102 E. Highland Avenue

CITY

Patton

STATE

CA

ZIP

92369

PRINTED NAME OF PERSON SIGNING

Janine Wallace

TITLE

Executive Director

CONTRACTING AGENCY AUTHORIZED SIGNATURE

DATE SIGNED

CALIFORNIA DEPARTMENT OF GENERAL SERVICES APPROVAL

EXEMPTION (If Applicable)

SCM Vol. I, 4.04 A.2.

EXHIBIT A
SCOPE OF WORK

1. CONTRACTED PARTIES:

- A. This Agreement is between County of San Bernardino on behalf of Arrowhead Regional Medical Center, hereafter referred to as the Contractor, and the Department of State Hospitals – Patton for the purpose of providing a clinical practicum experience for dietetic intern students, hereafter referred to as students.

2. SERVICE LOCATIONS:

- A. The services shall be performed at County of San Bernardino on behalf of Arrowhead Regional Medical Center, 400 N. Pepper Avenue, Colton, CA 92324.

3. SERVICE HOURS:

- A. The services shall be provided during the hours of 7:30 a.m. to 4:30 p.m., Monday through Friday, excluding state observed holidays, or as agreed upon by Contractor and Student.

4. PROJECT REPRESENTATIVES:

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

Contract Manager:

Department of State Hospitals – Patton	County of San Bernardino on behalf of Arrowhead Regional Medical Center
Section/Unit: Nutrition Services	Section/Unit: Nutrition Services
Attention: Jeanie Kim Dietetic Internship Program Director	Attention: Melanie Laoyan Supervising Dietitian
Address: 3102 E Highland Avenue Patton, CA 92369	Address: 400 N. Pepper Avenue Colton, CA 92324
Phone: (909) 672-1512 Fax: (909) 672-1582	Phone: (909) 580-2466 Fax: (909) 580-0003
Email: Jeanie.Kim@dsh.ca.gov	Email: LaoyanM@armc.sbcounty.gov

Administrative Contacts (all administrative inquiries should be directed to):

Department of State Hospitals – Patton	County of San Bernardino on behalf of Arrowhead Regional Medical Center
Section/Unit: Acquisitions & Contracts Unit	Section/Unit: Nutrition Services
Attention: Andrea Rocha Contracts Analyst	Attention: Melanie Laoyan Supervising Dietitian
Address: 3102 E Highland Avenue Patton, CA 92369	Address: 400 N. Pepper Avenue Colton, CA 92324
Phone: (909) 672-1503 Fax: (909) 425-7260	Phone: (909) 580-2466 Fax: (909) 580-0003
Email: andrea.rocha@dsh.ca.gov	Email: LaoyanM @armc.sbcounty.gov

Either party may make changes to the contact names or information above by giving written notice to the other party. Said changes shall not require an amendment to this Agreement.

5. SUMMARY OF WORK TO BE PERFORMED:

- A. Contractor shall provide clinical practicum experience for dietetic students in fulfilling requirements of the State's dietetic internship curriculum and professional development.

6. CONTRACTOR RESPONSIBILITIES:

- A. Contractor shall be committed to the advancement of the profession of dietetics in the fulfillment of its professionally and societal defined tasks on behalf of those whom it serves.
- B. Contractor shall provide a Registered Dietitian, commissioned through the Academy of Nutrition and Dietetics, to act as a Field Instructor for students placed for training. These instructors shall be afforded sufficient release time to instruct and supervise the student's work at the Contractor's facility in accordance with the educational objectives, learning experience, and performance expectations established by the DSH and agreed to by the Contractor.
- C. Contractor may request that the DSH remove any student whose performance the Contractor deems unfit to meet the demands of its service program or whose conduct otherwise interferes with its staff relationships or primary mission. Contractor may, however, remove a student when, in its opinion, the student poses an imminent threat to patient safety or welfare.
- D. Contractor shall provide facilities, staff, materials, and other resources necessary to meet the Contractor and the DSH educational commitments.
- E. Contractor shall accept students enrolled in the dietetic internship program at times, in numbers, and at such locations of the Contractor as shall be agreed upon by both parties.
- F. Contractor shall not use students to replace its regular staff and shall not require the students to render services except as they are identified for their learning value as part of an agreed upon educational program.
- G. Contractor shall not compensate students for their services unless otherwise and previously agreed to by the parties to this Agreement.
- H. Contractor and its subcontractors shall keep informed of, observe, comply with, and cause all of its agents and employees to observe and to comply with all prevailing Federal, State, and local laws, and rules and regulations made pursuant to said Federal, State, and local laws, which in any way affect the conduct of the work of this Agreement. If any conflict arises between provisions of the plans and specifications and any such law above referred to, then Contractor shall immediately notify the state in writing.
- I. DSH may terminate the Agreement pursuant to section 7 of Exhibit C if Contractor or its subcontractors fails to comply with a federal, state or local law and the noncompliance, based on the facts and circumstances, would constitute a material breach of this Agreement under California law.

7. STUDENT RESPONSIBILITIES:

- A. Student shall observe and respect all patient/client's rights, confidences, and dignity.

- B. Student shall dress in appropriate professional attire, as established by the Contractor and the DSH-P Dietetic Internship Program.
- C. Students must have DSH-P name tag on their person at all times.
- D. Student shall secure transportation and acquire living accommodations as necessary to participate in the clinical practicum experience.
- E. Student shall notify the Contractor and the DSH immediately whenever absence from the Contractor's facility becomes necessary.
- F. Student must show proof of current immunization for tetanus, diphtheria, Hepatitis B, measles, mumps, rubella, and polio; additionally, have had a skin test for tuberculosis within the past twelve months. Any exception to this certification provision shall be discussed with the Contractor prior to placement of the student in order to secure the Contractor's approval and acceptance of the student.
- G. Student shall show proof of Professional Liability insurance covering any damages caused by an error, omission or any negligent acts.
- H. Student must possess his/her own medical insurance coverage.

8. THE DSH RESPONSIBILITIES:

- A. The DSH shall assign a representative of its faculty to act as Field Instruction Consultant to the Contractor. The Consultant's responsibilities shall be to act as liaison between the Contractor and the DSH in the development and execution of the Field Instruction program and the evaluation of student performance, and to engage in such other activities as are of mutual concern in the provision of student training.
- B. The DSH, at the time of Agreement, shall provide the Contractor with a statement of its educational goals, of appropriate learning experiences, and of its expectations for student performance in the practicum. When and if necessary, that statement may be re-specified by mutual consent.
- C. The DSH shall be responsible for the selection, placement and/or removal, and final grading of students placed with the Contractor. These decisions shall be made in consultation with the Contractor with the respective responsibilities of each party to this Agreement.
- D. The DSH shall provide the Contractor with a medical statement from DSH-P Employee Clinic certifying that each student placed with the Contractor is physically fit to engage in Field Education.
- E. Rights of the DSH to Perform Quality Assurance and Reviews
 - i. The DSH may routinely evaluate the work performance of the Contractor and Students to ensure that all services are provided pursuant to the terms and conditions of this Agreement, standard of care, and the requirements of Title 22 of the California Code of Regulations (the "Standards").

Revision 8-9-19

EXHIBIT A-1
Student Privacy Acknowledgement and Nondisclosure
Agreement

I understand, while performing my duties as a student, I may have access to confidential information. I understand that confidential information is any information that identifies an individual, and that is created, maintained or used within the Department of State Hospitals (DSH) and may include medical information or personal information. Confidential information is information which is not available to the public. Special precautions are necessary to protect this type of information from unlawful or unauthorized access, use, modification, disclosure or destruction.

I agree to:

- Access, use or modify confidential information only as needed to perform my duties as a student.
- Never access or use confidential information out of curiosity, or for personal interest or advantage.
- Dispose of confidential information by utilizing the method of destruction approved by my supervisor. I will not dispose of such information in wastebaskets or recycle bins.
- Never show, discuss, or disclose confidential information to or with anyone who does not have the legal authority for access to the confidential information; this includes individuals who do not have a need to know this information.
- Never retaliate, coerce, threaten, intimidate or discriminate against or take other retaliatory actions against individuals or others who file complaints or participate in investigations or compliance reviews.
- Always store confidential information in a place physically secure from access by unauthorized persons.
- Never share passwords with anyone or store passwords in a location accessible to unauthorized persons.
- Always obtain proper authorization before removing confidential information from the work area.
- Follow all DSH privacy and security policies and procedures governing confidential information.

I certify that I understand that the privacy and security of information is strictly enforced and wrongful access, use or disclosure of confidential information is punishable as a crime and/or can result in disciplinary or civil action taken against me.

Print Full Name (First, Middle, Last)	Signature:
Agency/Department/School	Date Signed:

EXHIBIT A-2
Student and Instructor Requirements and Responsibilities

1. All students and instructors entering the Program must meet the following **HEALTH REQUIREMENTS**:

- A. Completion of the student health information form. This documentation substantiates the completion of the following vaccinations or tests:
 - i. Measles, Mumps, Rubella (MMR)
 - ii. Chickenpox history
 - iii. Tetanus (within the past 10 years)
 - iv. Hepatitis B vaccination series or initiation of the Hepatitis B vaccination series. Note: If the student chooses not to be vaccinated, a signed declination is required.
 - v. Annual influenza vaccination. Note: If the student chooses not to be vaccinated, a signed declination is required.
- B. All students and instructor(s) must provide DSH with documentation of two-step Tuberculin Skin Test (TST testing) by the Mantoux method. The first step is a TST result completed within the last 12 months prior to the date the Student and/or instructor is to provide services. The second step is a TST result completed within the last year prior to the date the Student and/or instructor is to provide services.

If both of the documented results of the TST's provided are less than or equal to 9mm of induration, then the student and/or instructor may be cleared to provide services. However, if the results of the TST's are greater than or equal to 10 mm of induration, then the students and/or instructor shall be subject to additional testing and/or clearances before s/he is allowed to provide services at DSH.

- i. If TST (purified protein derivative-PPD) is positive, a chest X-ray is required within the year.
 - ii. If the chest X-ray is positive, documentation of appropriate treatment must be provided.
 - iii. All students and instructors entering the Program will have the following **BACKGROUND CHECKS** conducted prior to beginning the first experiential education course and annually thereafter, as well as the criminal background check conducted by the DSH. The Contractor will provide the student's full name, driver's license number and date of birth to the DSH at least seven (7) to ten (10) days prior to the start of the rotation:
- C. Criminal Background Checks: A criminal background check will be requested from any state in which the individual has lived or worked in the previous ten (10) years (or since age 18, if under 28 years of age).

Exhibit A-2, Student and Instructor Requirements and Responsibilities

D. Name, Social Security Number, and Address Verification

2. All students and instructors entering the Program will be required to have Live Scan Fingerprinting completed. This documentation must be provided to the DSH prior to the start of the rotation.
3. All students and instructors will receive instruction on the importance of maintaining patient privacy and confidentiality and the local, state and federal laws governing patient confidentiality, including but not limited to, the Health Insurance Portability and Accountability Act (HIPAA) of 1996.
4. All students and instructors will receive basic instruction on Occupational Safety and Health Administration (OSHA) rules and regulations as they relate to their field of study.
5. All students and instructors must complete and be certified in **BASIC LIFE SUPPORT** (Adult CPR) prior to starting clinical work practice experiences.
6. All students and instructors are required to possess their own medical coverage.
7. All students and instructors must comply with DSH's administrative policies, procedures, rules and regulations;
8. All students and instructors must comply with DSH's dress code and wear DSH issued badge identifying themselves;
9. All students and instructors are responsible for attending an orientation to be provided by DSH;
10. All students and instructors are responsible for notifying the DSH Contract Manager or designee immediately of any violation of state or federal laws by any student; and
11. All students and instructors are responsible for providing services to DSH's clients only under the direct supervision of DSH's professional staff.
12. All students and instructors are responsible for maintaining the confidentiality of client information.
 - A. No student or instructor shall have access to or have the right to receive any client record, except when necessary in the regular course of the placement experience. The discussion, transmission, or narration in any form by students of any individually identifiable client information, medical or otherwise, obtained in the course of the Program is forbidden except as a necessary part of the practical experience.
 - B. Neither Contractor nor its employees or agents shall be granted access to individually identifiable information unless the client has first given consent using a form approved by DSH that complies with applicable state and federal law, including the Health Insurance Portability and Accountability Act ("HIPAA") and its implementing regulations.
13. Students and instructors are not employees or agents of the Contractor, nor the DSH and shall receive no compensation for their participation in the Program, either from Contractor, nor the DSH. For purposes of this Agreement, however, students are trainees and shall be considered members of DSH's "workforce" as that term is defined by the HIPAA regulations at 45 C.F.R. § 160.103.

EXHIBIT B
BUDGET DETAIL AND PAYMENT PROVISIONS

- A. This is a zero (\$0.00) dollar agreement. By the Contractor accepting this agreement at no cost, the State has no further obligations or hidden costs associated with acceptance.
- B. The Contractor shall not be reimbursed for student and/or instructor travel-related expenses. All travel shall be at the expense of student and/or instructor.

EXHIBIT D
SPECIAL TERMS AND CONDITIONS
INTERAGENCY AGREEMENT

1. TERMINATION:

- A. Either party may terminate this Agreement by giving 30 days written notice to the other party. The notice of termination shall specify the effective date of termination. Upon the Contractor's receipt of notice of termination from the Department of State Hospitals (DSH), and except as otherwise directed in the notice, the Contractor shall:
- a. Stop work on the date specified in the notice;
 - b. Place no further orders or enter into any further subcontracts for materials, services or facilities except as necessary to complete work under the Agreement up to effective date of termination;
 - c. Terminate all orders and subcontracts;
 - d. Promptly take all other reasonable and feasible steps to minimize any additional cost, loss, or expenditure associated with work terminated, including, but not limited to reasonable settlement of all outstanding liability and claims arising out of termination of orders and subcontracts;
 - e. Deliver or make available to DSH all data, drawings, specifications, reports, estimates, summaries, and such other information and materials as may have been accumulated by the Contractor under this Agreement, whether completed, partially completed, or in progress.
- B. In the event of termination, an equitable adjustment in the price provided for this Agreement shall be made. Such adjustment shall include reasonable compensation for all services rendered, materials supplies, and expenses incurred pursuant to this Agreement prior to the effective date of termination.

2. DISPUTES:

- A. Contractor shall first discuss and attempt to resolve any dispute arising under or relating to the performance of this Agreement.

3. CHANGES IN TIME FOR PERFORMANCE OF TASKS:

- A. The time for performance of the tasks and items within the budget, but not the total agreement price, may be changed with the prior written approval of the Contract Manager. However, the date for completion of performance and the total agreement price, as well as all other terms not specifically accepted may be altered only by formal amendment of this Agreement.

4. APPROVAL OF PRODUCT:

- A. Each product to be approved under this Agreement shall be approved by the Contract Manager. The DSH's determination as to satisfactory work shall be final, absent fraud or mistake.

5. AGREEMENT IS COMPLETE:

- A. Other than as specified herein, no document or communication passing between the parties hereto shall be deemed a part of this Agreement.

6. CAPTIONS:

- A. The clause headings appearing in this Agreement have been inserted for the purpose of convenience and ready reference. They do not purport to and shall not be deemed to define, limit or extend the scope or intent of the clauses to which they pertain.

7. PUBLIC HEARINGS:

- A. If public hearings on the subject matter dealt with in this Agreement are held within one year from the Agreement expiration date, Contractor shall make available to testify the personnel assigned to this Agreement at the hourly rates specified in the Contractor's proposed budget. The DSH shall reimburse Contractor for travel of said personnel at the Agreement, or if none, at State rates for such testimony as may be requested by the DSH.

8. FORCE MAJEURE:

- A. Neither the DSH nor the Contractor shall be deemed to be in default in the performance of the terms of this Agreement if either party is prevented from performing the terms of this Agreement by causes beyond its control, which shall include without being limited to: acts of God; interference, rulings or decision by municipal, Federal, State or other governmental agencies, boards or commissions; any laws and/or regulations of such municipal, State, Federal, or other governmental bodies; or any catastrophe resulting from flood, fire, explosion, earthquakes or other similar environmental causes beyond the control of the defaulting party. If any of the stated contingencies occur, the party delayed by force majeure shall immediately give the other party written notice of the cause of delay. The party delayed by force majeure shall use reasonable diligence to correct the cause of the delay, if correctable.

9. SEVERABILITY:

- A. If any provision of this Agreement is held invalid by a court of competent jurisdiction, such invalidity shall not affect any other provision of this Agreement and remainder of this Agreement shall remain in full force and effect. Therefore, the provisions of this Agreement are and shall be deemed to be severable.

10. CLIENT CONFIDENTIALITY:

- A. For an Agreement involving clients and information regarding clients, the Contractor shall protect from unauthorized disclosure, names and other identifying information concerning persons receiving services pursuant to this Agreement, except for statistical information not identifying any client. Client is defined as "those persons receiving services pursuant to a DSH funded program." Contractor shall not use such identifying information for any purpose other than carrying out the Contractor's obligations under this Agreement.
- B. Contractor shall promptly transmit to the DSH all requests for disclosure of such identifying information not emanating from the client. Contractor shall not disclose, except as otherwise

Exhibit D, Special Terms and Conditions Interagency Agreement

specifically permitted by this Agreement or authorized by the client, any such identifying information to anyone other than the DSH without prior written authorization from DSH.

- C. For purposes of this section, identity shall include but not be limited to name, identifying number, symbol or other identifying piece of information assigned to the individual, such as a finger or voice print or a photograph which can be used to identify the individual person.

Department of State Hospitals
Patton

County of San Bernardino on behalf of Arrowhead Regional Medical Center
Agreement Number: 21-30049-000
Exhibit E, Confidentiality and Information Security Provisions
(HIPAA Business Associate Agreement)

EXHIBIT E
CONFIDENTIALITY AND INFORMATION SECURITY PROVISIONS
(HIPAA Business Associate Agreement)

This Exhibit E is not applicable to this Agreement.

Revision 8-1-19

EXHIBIT F
INFORMATION PRIVACY AND SECURITY REQUIREMENTS
(Non-HIPAA/HITECH Act Contracts)

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

- I. Order of Precedence: With respect to information privacy and security requirements for all DSH 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 DSH, 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 DSH PCI disclosed to Contractor, or collected, created, maintained, stored, transmitted or used by Contractor for or on behalf of DSH, pursuant to Contractor's agreement with DSH. 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 DSH, including this Exhibit, the following definitions shall apply:
 - A. Breach: "Breach" means:
 1. the unauthorized acquisition, access, use, or disclosure of DSH PCI in a manner which compromises the security, confidentiality or integrity of the information; or
 2. the same as the definition of "breach of the security of the system" set forth in California Civil Code section 1798.29(f).
 - B. Confidential Information: "Confidential information" means information that:
 1. does not meet the definition of "public records" set forth in California Government Code section 6252(e), or is exempt from disclosure under any of the provisions of Section 6250, et seq of the California Government Code or any other applicable state or federal laws; or
 2. is contained in documents, files, folders, books or records that are clearly labeled, marked or designated with the word "confidential" by DSH.
 - 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" collectively (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 DSH PCI, in violation of any state or federal law or in a manner not permitted under the agreement between Contractor and DSH, 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 DSH 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 DSH PCI. The Contractor shall not disclose, except as otherwise specifically permitted by the agreement between Contractor and DSH (including this Exhibit), any DSH

PCI to anyone other than DSH personnel or programs without prior written authorization from the DSH 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 DSH PCI for any purpose other than performing the Contractor's obligations under its agreement with DSH.
- VI. Safeguards: The Contractor shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the privacy, confidentiality, security, integrity, and availability of DSH PCI, including electronic or computerized DSH PCI. At each location where DSH 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 DSH, including this Exhibit, and which incorporates the requirements of Section VII, Security, below. Contractor shall provide DSH with Contractor's current and updated policies within five (5) business days of a request by DSH 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 DSH 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 DSH PCI is located, the Contractor shall designate a Security Officer to oversee its compliance with this Exhibit and to communicate with DSH 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 DSH, including this Exhibit, or otherwise use or disclose DSH 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 DSH inspection for a period of three years following contract termination or completion.
 - C. Contractor shall provide DSH with its employee's certifications within five (5) business days of a request by DSH 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.
- XI. Breach and Security Incident Responsibilities:
 - A. Notification to DSH of Breach or Security Incident: The Contractor shall notify DSH **immediately by telephone call plus email or fax** upon the discovery of a breach (as defined in this Exhibit), **and within twenty-four (24) hours by email or fax** of the discovery of any security incident (as defined in this Exhibit), unless a law enforcement agency determines that the notification will impede a criminal investigation, in which case the notification required by this section shall be made

to DSH immediately after the law enforcement agency determines that such notification will not compromise the investigation. Notification shall be provided to the DSH Program Contract Manager, the DSH Privacy Officer and the DSH 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 DSH PCI in electronic or computerized form, notification to DSH shall be provided by calling the DSH 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 and 1798.82.

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 DSH Program Contract Manager, the DSH Privacy Officer, and the DSH Chief Information Security Officer of:

1. what data elements were involved, and the extent of the data disclosure or access involved in the breach, including, specifically, the number of individuals whose personal information was breached; and
2. a description of the unauthorized persons known or reasonably believed to have improperly used the DSH PCI and/or a description of the unauthorized persons known or reasonably believed to have improperly accessed or acquired the DSH PCI, or to whom it is known or reasonably believed to have had the DSH PCI improperly disclosed to them; and
3. a description of where the DSH PCI is believed to have been improperly used or disclosed; and
4. a description of the probable and proximate causes of the breach or security incident; and
5. whether Civil Code section 1798.29 and 1798.82 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 DSH Program Contract Manager, the DSH Privacy Officer, and the DSH 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 DSH PCI, Contractor shall, at its sole expense, and at the sole election of DSH, 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 DSH 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 DSH 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 or 1798.82, and regardless of whether Contractor is considered only a custodian and/or non-owner of the DSH PCI, Contractor shall, at its sole expense, and at the sole election of DSH, 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), or 1798.82, subdivision (f). Contractor shall inform the DSH 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 DSH in its submission of a sample copy of the notification to the Attorney General.
- F. DSH Contact Information: To direct communications to the above referenced DSH staff, the Contractor shall initiate contact as indicated herein. DSH 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.

DSH Program Contract Manager	DSH Privacy Officer	DSH Chief Information Security Officer
See the Scope of Work exhibit for Program Contract Manager	Privacy Officer Office of Legal Services California Dept. State Hospitals 1600 9 th Street, Room 433 Sacramento, CA 95814 Email: yamin.scardigli@DSH.ca.gov Telephone: (916) 562-3721	Chief Information Security Officer Information Security Office 1600 9th Street, Suite 250 Sacramento, CA 95814 Email: iso@dsh.ca.gov and security@dsh.ca.gov Telephone: (916) 654-4218

- XII. Documentation of Disclosures for Requests for Accounting: Contractor shall document and make available to DSH or (at the direction of DSH) to an Individual such disclosures of DSH 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 DSH PCI by Third Parties: The Contractor and its employees, agents, or subcontractors shall promptly transmit to the DSH Program Contract Manager all requests for disclosure of any DSH PCI requested by third parties to the agreement between Contractor and DSH (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: DSH 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 DSH Program Contract Manager in writing.
- XV. Return or Destruction of DSH PCI on Expiration or Termination: Upon expiration or termination of the agreement between Contractor and DSH for any reason, Contractor shall securely return or destroy the DSH PCI. If return or destruction is not feasible, Contractor shall provide a written explanation to the DSH Program Contract Manager, the DSH Privacy Officer and the DSH 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, DSH 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 destroys the DSH PCI or returns the DSH PCI to DSH; provided however, that on expiration or termination of the agreement between Contractor and DSH, Contractor shall not further use or disclose the DSH PCI except as required by state or federal law.
- C. Notification of Election to Destroy DSH PCI: If Contractor elects to destroy the DSH PCI, Contractor shall certify in writing within 30 days of the expiration or termination of the agreement to the DSH Program Contract Manager, the DSH Privacy Officer and the DSH Chief Information Security Officer, using the contact information listed in Section XI(F), above, that the DSH 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 DSH 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 DSH, available to DSH at no cost to DSH to testify as witnesses, in the event of litigation or administrative proceedings being commenced against DSH, 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 DSH 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 DSH PCI upon the expiration 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 DSH.

Attachment 1
Contractor Data Security Standards

1. General Security Controls

- A. **Confidentiality Statement.** All persons that will be working with DSH PCI must sign a confidentiality statement. The statement must include at a minimum, General Use, Security and Privacy safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to DSH PCI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for DSH inspection for a period of three (3) years following contract termination.
- B. **Background check.** Before a member of the Contractor's workforce may access DSH PCI, Contractor must conduct a thorough background check of that worker and evaluate the results to assure that there is no indication that the worker may present a risk for theft of confidential data. The Contractor shall retain each workforce member's background check documentation for a period of three (3) years following contract termination.
- C. **Workstation/Laptop encryption.** All workstations and laptops that process and/or store DSH PCI must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher. The encryption solution must be full disk unless approved by the DSH Information Security Office.
- D. **Server Security.** Servers containing unencrypted DSH PCI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.
- E. **Minimum Necessary.** Only the minimum necessary amount of DSH PCI required to perform necessary business functions may be copied, downloaded, or exported.
- F. **Removable media devices.** All electronic files that contain DSH PCI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, smart devices tapes etc.). PCI must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher
- G. **Antivirus software.** All workstations, laptops and other systems that process and/or store DSH PCI must install and actively use a comprehensive anti-virus software solution with automatic updates scheduled at least daily.
- H. **Patch Management.** All workstations, laptops and other systems that process and/or store DSH PCI must have operating system and application security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release.
- I. **User IDs and Password Controls.** All users must be issued a unique user name for accessing DSH PCI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password. Passwords are not to be shared. Must be at least eight characters. Must be a non-dictionary word. Must not be stored in readable format on the computer. Must be changed every 60 days. Must be changed if revealed or

compromised. Must be composed of characters from at least three of the following four groups from the standard keyboard:

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

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

2. System Security Controls

- A. **System Timeout.** The system must provide an automatic timeout, requiring reauthentication of the user session after no more than 20 minutes of inactivity.
- B. **Warning Banners.** All systems containing DSH PCI must display a warning banner each time a user attempts access, stating that data is confidential, systems are logged, and system use is for business purposes only. User must be directed to log off the system if they do not agree with these requirements.
- C. **System Logging.** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for DSH PCI, or which alters DSH PCI. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. This logging must be included for all user privilege levels including, but not limited to, systems administrators. If DSH PCI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.
- D. **Access Controls.** The system must use role based access controls for all user authentications, enforcing the principle of least privilege.
- E. **Transmission encryption.** All data transmissions of DSH PCI outside the contractor's secure internal network must be encrypted using a FIPS 140-2 certified algorithm, such as Advanced Encryption Standard (AES), with a 128bit key or higher. Encryption can be end to end at the network level, or the data files containing DSH PCI can be encrypted. This requirement pertains to any type of DSH PCI in motion such as website access, file transfer, and E-Mail.
- F. **Intrusion Detection.** All systems involved in accessing, holding, transporting, and protecting DSH PCI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

3. Audit Controls

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

- B. **Log Reviews.** All systems processing and/or storing DSH PCI must have a routine procedure in place to review system logs for unauthorized access.
- C. **Change Control.** All systems processing and/or storing DSH PCI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

4. Business Continuity / Disaster Recovery Controls

- A. **Disaster Recovery.** Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic DSH PCI in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this agreement for more than 24 hours.
- B. **Data Backup Plan.** Contractor must have established documented procedures to securely backup DSH PCI to maintain retrievable exact copies of DSH PCI. The backups shall be encrypted. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and the amount of time to restore DSH PCI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of DSH data.

5. Paper Document Controls

- A. **Supervision of Data.** DSH PCI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. DSH PCI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.
- B. **Escorting Visitors.** Visitors to areas where DSH PCI is contained shall be escorted and DSH PHI shall be kept out of sight while visitors are in the area.
- C. **Confidential Destruction.** DSH PCI must be disposed of through confidential means, using NIST Special Publication 800-88 standard methods for data sanitization when the DSH PSCI is no longer needed.
- D. **Removal of Data.** DSH PCI must not be removed from the premises of the Contractor except with express written permission of DSH.
- E. **Faxing.** Faxes containing DSH PCI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending.
- F. **Mailing.** DSH PCI shall only be mailed using secure methods. Large volume mailings of DSH PHI shall be by a secure, bonded courier with signature required on receipt. Disks and other transportable media sent through the mail must be encrypted with a DSH approved solution, such as a solution using a vendor product specified on the CALIFORNIA STRATEGIC SOURCING INITIATIVE.