

STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES

**STANDARD AGREEMENT**

STD 213 (Rev. 03/2019)

AGREEMENT NUMBER

19-11089

PURCHASING AUTHORITY NUMBER (If Applicable)

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

CONTRACTING AGENCY NAME

California Department of Public Health

CONTRACTOR NAME

Cardinal Health Pharmacy Services, LLC

2. The term of this Agreement is:

START DATE

04/14/2020

THROUGH END DATE

09/30/2020

3. The maximum amount of this Agreement is:

\$500,000.00

Five Hundred Thousand 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	Pharmacy Agreement	28
Attachment 1	HIPAA BAA	14
+		
-		

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.)

Cardinal Health Pharmacy Services, LLC

CONTRACTOR BUSINESS ADDRESS

13651 Dublin Court

CITY

Stafford

STATE

TX

ZIP

77477

PRINTED NAME OF PERSON SIGNING

Mike Brown

TITLE

VP, Pharmacy Operations and Account Mngmt

CONTRACTOR AUTHORIZED SIGNATURE

Michael Michael D. Brown

Michael D. Brown (Apr 16, 2020)

DATE SIGNED

Apr 16, 2020

**STATE OF CALIFORNIA**

CONTRACTING AGENCY NAME

California Department of Public Health

CONTRACTING AGENCY ADDRESS

1615 Capitol Ave

CITY

Sacramento

STATE

CA

ZIP

95814

PRINTED NAME OF PERSON SIGNING

Tim Bow

TITLE

Procurement Officer

CONTRACTING AGENCY AUTHORIZED SIGNATURE

Timothy Bow

Digitally signed by Timothy Bow  
Date: 2020.04.15 14:40:23 -07'00'

DATE SIGNED

CALIFORNIA DEPARTMENT OF GENERAL SERVICES APPROVAL

EXEMPTION (If Applicable)

PCC 1102

Executive Order N-25-20-COVID-19

This Pharmacy Agreement ("Agreement") is entered into by and between Cardinal Health Pharmacy Services, LLC, located at 13651 Dublin Ct., Stafford, Texas 77477 ("Cardinal Health") and California Department of Public Health, located at 1616 Capitol Avenue, Sacramento, California 95814 ("Customer"). Cardinal Health and the Customer shall each be referred to a "Party" or collectively as the "Parties".

## **RECITALS**

- A. WHEREAS, the State determined that grounds exist to contract with an operator to provide critical and "essential" medical services, pursuant to the Governor's Proclamation of a State of Emergency dated March 4, 2020, and the Governor's Emergency Declaration, Executive Order (EO) N-25-20 dated March 12, 2020, as amended or supplemented subsequently (collectively, the "Executive Orders"). The State also finds that the use and operation of alternative care facilities is necessary to mitigate the effects of the COVID-19 emergency.
- B. WHEREAS, all agencies of the state government shall perform any and all activities consistent with the direction of the State, pursuant to the Executive Order.
- C. WHEREAS, Cardinal Health shall be the exclusive provider of the pharmacy services set forth in this Agreement for Customer's pharmacy operations ("Pharmacy"), at the temporary Alternative Care Facility ("ACF") located at the Sleep Train Arena, 1 Sports Pkwy, Sacramento, CA 95834.
- D. WHEREAS, the State selected the ACF as a location for the enhanced availability of hospital beds and space to be used by the State or its designated agencies for inpatient medical services associated with the COVID-19 pandemic. The State selected Cardinal Health to operate and maintain the Pharmacy (as described below) for patients admitted to the ACF during the novel coronavirus outbreak.
- E. WHEREAS, as of the Agreement Date, Cardinal Health will initiate pharmacy operations at the ACF, pursuant to the terms of this Agreement and applicable State and Federal law,
- F. WHEREAS, the parties wish to document their Agreement with respect to the provision of such services between Cardinal Health and the State.

NOW, THEREFORE, in consideration of the facts referenced above and the covenants contained herein, it is hereby agreed as follows:

## **ARTICLE I DUTIES**

**1.01 Cardinal Health Duties.** With Customer's cooperation, Cardinal Health shall provide patient care-oriented pharmacy services to the ACF with knowledge and expertise of the accreditation standards for pharmaceutical services of The Joint Commission ("TJC") or other accrediting agency as may be applicable, as well as Medicare and Medicaid conditions of participation and applicable law.

a. **Pharmacy Personnel.** Cardinal Health shall provide one (1) onsite full-time project manager and one (1) onsite full-time pharmacist-in-charge + director of pharmacy ("PIC/DOP") to set-up and manage the Pharmacy at the ACF with specific duties and responsibilities as follows:

i. The PIC/DOP shall:

- (1) Manage the Pharmacy staff, including the activities and performance of pharmacists and technicians and any students and interns
- (2) Assure adequate control and documentation of controlled substances

- (3) Support and oversee the preparation and delivery of medication throughout the ACF pursuant to processes established by Customer
- (4) Report to the Customer issues concerning the development and maintenance of the information systems and other technology applications within the Pharmacy and assist with implementing repairs as reasonably requested
- (5) Lead Pharmacy meetings
- (6) Participate in the ACF committee, policy or leadership meetings, as applicable
- (7) Identify areas for quality and safety improvements and suggest which areas take priority
- (8) Perform staff pharmacist duties, as necessary
- (9) Responsible for the storage of drugs and all drug storage areas, and for the disposal of drugs in accordance with all applicable Federal, State and local laws and requirements.
- (10) Assist Customer in Pharmacy closure, including but not limited to drug and narcotic disposal, return to vendor or use of a reverse distributor for crediting purposes to Customer's accounts, assuring all accountability documents are organized and secured and reporting on Pharmacy status and inventory of supplies, equipment and hours and schedule of Pharmacy staff.
- (11) Oversee the ordering of drugs and pharmaceutical supplies in accordance with the established processes of the Customer
- (12) Support Cardinal Health Remote Pharmacy Services in the implementation services as needed
- (13) Coordinate with Customer to obtain appropriate licensures, waivers or clearances.
- (14) Adhere to Customer's policies and procedures and comply with Customer's requirements related to risk management, safety, security, fire, and infection control. Comply with all applicable State, local and Federal laws and requirements during the term of the Agreement.

ii. The Project Manager shall:

- (1) Set up, develop and implement processes for the Pharmacy and pharmacy operations and for the preparation and delivery of medication throughout the ACF or Customer's additional alternative care facilities
- (2) Develop and implement processes for the adequate control and documentation of controlled substances
- (3) Report to the Customer's leadership issues concerning the development and maintenance of the information systems and other technology applications for pharmacy operations at the ACF or at additional alternative care facilities, and to assist with implementing repairs as reasonably requested
- (4) Participate in committee, policy or leadership meetings, as applicable
- (5) Lead Pharmacy meetings
- (6) Identify areas for quality and safety improvements and suggest which areas take priority
- (7) Support Cardinal Health Remote Pharmacy Services in the implementation of services as needed
- (8) Coordinate with Customer to obtain appropriate licensures, waivers or clearances
- (9) Oversee the ordering of drugs and pharmaceutical supplies in accordance with the established processes of the Customer.
- (10) Develop and implement staffing and workflow model

- (11) Assist Customer in the recruitment and hiring of pharmacy staff that meet or exceed the minimum required competency standards
- (12) Develop, implement and update as needed pharmacy and medication policies and procedures, including but not limited to procedures for handling drug recalls
- (13) Collaborate with Customer's leadership and personnel, and assist with the development of orientation presentations and materials for new hires
- (14) Upon Customer's request and pursuant to arrangement between Cardinal Health and Customer, travel to other alternative care facilities of the Customer to perform the duties set forth herein and oversee the implementation, operations and management of the pharmacies at such alternative care facilities
- (15) Adhere to Customer's policies and procedures and comply with Customer's requirements related to risk management, safety, security, fire, and infection control. Comply with all applicable State, local and Federal laws and requirements during the term of the Agreement.

**b. Staff Training and Development.** Cardinal Health shall provide education materials for Pharmacy personnel, and upon request, for the ACF physicians, nurses and other employees on current and emerging pharmacy issues as requested by Customer. Such materials may include: (i) routine updates regarding drug therapies; (ii) new product evaluation; (iii) review of specific therapeutic categories; (iv) strategies for controlling drug costs; and (v) material and information to address patient safety concerns including medication error prevention strategies, adverse drug events and other important drug therapy related topics. At the request of the Customer, Cardinal Health agrees to:

- i. Participate in ACF and pharmacy orientation for new hires; and
- ii. Oversee the standards and training of pharmacy staff on sterile product preparation in compliance with USP 795/797/800 non-sterile and sterile preparation standards

**c. Pharmacy & Therapeutics Committee.** If applicable, the PIC/DOP, or designee, shall participate on ACF's committee that performs Pharmacy and Therapeutic review functions.

**d. Clinical Services.** Cardinal Health shall provide clinical strategies customized to meet the ACF's needs using proprietary tools and publications. Such services shall include:

- i. Optimize drug use to promote safe and effective drug therapy
- ii. Provide evidence-based strategies for the provision of clinical initiatives
- iii. Provide Cardinal Health clinical subject matter expert/clinical director to monitor system and recommend actions to Customer's or ACF staff

**e. Pharmacy Clinical and Quality Resources.** Cardinal Health Project Manager and/or subject matter experts shall provide clinical and quality-related documents and resources when available.

- i. Clinical resources include evidence-based clinical information
- ii. Quality resources include:
  - (1) Access to *Quality Matters!*, a monthly electronic newsletter for conducting educational in-service programs
  - (2) Generic policies and procedure related to quality issues that may be used as starting templates
  - (3) URL links to quality, medication safety, regulatory, and accreditation resources

**f. Patient Safety.** Cardinal Health shall support the ACF's compliance with National Patient Safety ("NPS") goals in effect at the time.

**g. Reports.** Cardinal Health shall provide reports, if applicable, measuring operational, financial and clinical progress towards goals in its customary form.

**h. Pharmacy Inventory Management.** Cardinal Health shall manage the Pharmacy's inventory and drug procurement at the ACF in accordance with Customer's established inventory and drug procurement processes and industry standards. Cardinal Health's inventory management responsibilities shall also include monthly inspections for out-of-date drugs and short-date drugs processed for return credit when available, management of breakage, shrinkage and loss, maximization of inventory turns and minimization of stock outs in accordance with industry standards. A perpetual inventory shall not be maintained, except as required for controlled substances by applicable law.

**i. Order Drugs.** Cardinal Health shall oversee the ordering of all drugs through Customer's wholesale distributor contract and procurement process for drugs and pharmaceutical supplies at the ACF.

**j. Pharmacy Operations.** The Pharmacy shall be open twenty-four hours a day, seven days a week ("24/7"). Any changes in the Pharmacy's hours of operation or number of full-time equivalent employees required may be considered a change of service, which may require renegotiation of this Agreement. Therefore, any such change must be mutually agreed to in writing between the Parties.

**k. Remote Pharmacy Services.** Cardinal Health shall provide four and one-half (4.5) full-time equivalent ("FTE") dedicated remote pharmacists to enter physician medication orders (the "Remote Pharmacy Services"). The Remote Pharmacy Services as well as the applicable terms and conditions related to this service are further detailed in Exhibit A, attached hereto and incorporated by reference herein. Customer may request that Cardinal Health increase the number of FTE upon one (1) weeks' prior written notice and may request that Cardinal Health decrease the number of FTE upon two (2) weeks' prior written notice. Notification shall be from individuals referred to in the Notices section below.

**l. Additional Services.** If Customer requests Cardinal Health to provide additional services which require additional resources prior to execution of a further written agreement, Cardinal Health shall charge Customer its usual and customary fee for such additional service.

**1.02 Customer Duties.** The Parties agree that Cardinal Health's success is predicated upon Customer's cooperation, facilitation, and timely implementation of recommended or agreed upon initiatives. As such, Customer agrees to perform the following:

**a. Licensure and Permits.** Customer, with Cardinal Health's assistance, shall obtain all necessary local, state and federal licenses and permits required for the operation of the Pharmacy and shall have the primary responsibility for record keeping and security of controlled substances maintained within its premises, including the Pharmacy.

**b. Grant of Authority.** Customer shall allow Cardinal Health to act in its name, to the extent permitted by law, and to the extent necessary to enable Cardinal Health to perform under this Agreement, under permits issued in Customer's name by the applicable state Board of Pharmacy, Drug Enforcement Administration, and other governmental health care regulatory agencies that affect the operation of pharmacies. Customer shall issue a Power of Attorney to Cardinal Health for the sole purposes of ordering and purchasing controlled substances on its behalf for use at the ACF.

**c. Cooperation.** Customer shall actively support and require Customer's employees, agents and staff to (a) cooperate with Cardinal Health's management of the Pharmacy as required by this Agreement; and (b) use and support cost containment and quality measurement tools reasonably requested by Cardinal Health. If Customer or its employees, agents or staff fail to cooperate or use and support such tools, Cardinal Health reserves the right to adjust and/or modify its fees.

**d. Employees.** All employees of the Pharmacy not referenced in Section 1.01(a) shall be employees or agents of Customer. Unless otherwise agreed in writing, Customer shall, for the term of this Agreement and any extension thereof, provide the services of at least the same number of full-time equivalent registered pharmacists and support personnel that staffed the Pharmacy immediately preceding the operation of the ACF. Such additional personnel may be required to support increased services, regulatory requirements and

changes to operational hours. Customer shall be responsible for recruitment and final selection for all Pharmacy employees.

**e. Plant, Property, Supplies and Equipment**

- i. Customer shall retain responsibility for the Pharmacy's physical plant and compliance with applicable federal and state laws, regulations and guidelines related thereto, including environmental safety training required by applicable law. Customer is responsible for implementing and maintaining information technology systems necessary for continued Pharmacy operations, including any personnel required for such implementation and maintenance. Customer shall provide fixed and movable Pharmacy equipment, including maintenance required for the efficient operation of the Pharmacy.
- ii. Customer shall provide "Other Items" as necessary and customary for the successful operation of the Pharmacy, including but not limited to reasonable office equipment, supplies, dues and subscriptions, publications, and non-drug pharmaceutical supplies used in preparation, packaging or storing of drugs and any items that Parties mutually agree is necessary for the successful operation of the Pharmacy. If Customer is unable to provide, Cardinal Health shall purchase such items on behalf of Customer and pass the expenses through to Customer pursuant to Section 3.01(c).

**f. Information Technology.** Customer shall provide computers that meet the hardware and software requirements of wholesaler and other vendors.

**g. Credit Information.** Customer shall provide Cardinal Health with any credit information prior to the start of the services set forth in this Agreement and, after that, as may be reasonably requested by Cardinal Health from time to time. Notwithstanding the foregoing, Customer shall not have to provide any credit information if it is a department/agency of the State of California.

**h. Invoice Payment.** Customer shall be responsible for the payment of all drug invoices, (even though such drugs were ordered by Cardinal Health on behalf of Customer for the ACF) together with all applicable sales, use, excise, gross receipts, or other federal, state, or local taxes or other assessments, on its purchase of taxable drugs.

**ARTICLE II  
LICENSURE AND REGULATORY REQUIREMENTS**

**2.01** Services provided shall comply with all applicable laws, ordinances, regulations and standards of all applicable accrediting bodies, in effect during the term of this Agreement, as well as those written policies of the ACF made available to Cardinal Health, including those related to risk management, safety, security, fire, and infection control.

**2.02** All pharmacists who dispense Drugs shall be duly licensed as pharmacists as required under the laws of the state in which Customer is located. In addition, all Customer's employees, agents and staff who provide patient services shall be certified and/or licensed and in good standing as required by the laws of the state in which Customer is located. Each Party shall immediately notify the other should this status change.

**2.03** Neither Party is excluded nor disqualified in any manner from participation in any federally-funded health care program. Each Party shall notify the other party as soon as possible should this status change.

**2.04** Each Party covenants that it is in good standing under the laws of the state in which it is organized and has the power and authority to enter into this Agreement. Each Party shall immediately notify the other should this status change.

**ARTICLE III  
COMPENSATION AND FINANCIAL ARRANGEMENTS**

**3.01.** Cardinal Health shall invoice Customer and Customer shall pay Cardinal Health for the following services set forth below:

a. **Monthly Management Fee.** A monthly fee in the amount of sixty-five thousand dollars (\$65,000) ("Management Fee"). Services provided for one or more days in any given month shall be subject to the full amount of the Management Fee. Following the Initial Term (defined below) and provided that the services of the PIC/DOC are no longer necessary at the ACF or any other Alternative Care Facility operated by Customer, Cardinal Health agrees the Management Fee shall be reduced to \$50,000 per month for services provided by the Project Manager only.

b. **Salary, Wages and Benefits.** Cardinal Health's actual cost of the PIC/DOP's salary, wages, and benefits, including productive and non-productive time and deferred compensation (retention bonuses) not to exceed \$20,000 per month.

c. **Other Items.** Should the Customer be unable to supply an item as defined in Section 1.02(e), then Cardinal Health shall purchase and pass through the item at invoice cost.

d. **Travel Expenses.** Project manager's and PIC/DOP's travel expenses shall be passed through to Customer.

e. **Remote Pharmacy Services ("RPS") Fees.**

i. **RPS Start-up Fee.** Customer agrees to pay Cardinal Health a one-time Start-Up Fee in the amount of eight thousand five hundred dollars (\$8,500).

ii. **Monthly RPS Fee.** Customer agrees to pay Cardinal Health a Monthly RPS Fee in the amount of seventeen thousand dollars (\$17,000) per month per full-time RPS pharmacist.

f. **Taxes.** Customer shall pay all sales, use, excise, gross receipts, or other federal, state, or local taxes (other than taxes based solely on the net income of Cardinal Health) in connection with or arising out of the transactions contemplated by this Agreement and shall reimburse Cardinal Health for any and all costs associated with any Cardinal Health payment on Customer's behalf, including, without limitation, any interest, penalties, audit costs or attorney's fees. If Customer is exempt from sales, use, excise, gross receipts, or other federal, state, or local taxes, Customer shall provide documentation of such exemption to Cardinal Health. Customer shall immediately notify Cardinal Health, in writing, of any change in its tax status. If Customer's exempt status is challenged by any jurisdiction, Customer shall be solely responsible for resolving any such dispute and shall immediately notify Cardinal Health of the dispute. Customer shall hold Cardinal Health harmless and reimburse any expenses that Cardinal Health may incur as a result of any such challenge.

**3.02. Payment Terms.**

a. Cardinal Health shall provide an estimated invoice to Customer each calendar month for the pharmacy services listed in section 3.01(a) – (e) to be provided during the following Service Month pursuant to this Agreement, and any applicable credits or debits arising from the reconciliation of the prior Service Month's actual invoice to the estimated invoice. (A Service Month is defined as the month in which services are rendered to the Customer.) Cardinal Health shall provide such estimated invoice fifteen (15) days prior to each Service Month

b. Each Cardinal Health invoice shall contain the following:

Agreement # XX-XXXXX  
Attention:  
California Department of Public Health  
Center for Health Care Quality, Licensing and Certification Program

MS 3001  
PO Box 997377  
Sacramento, CA 95899-7377

c. All documentation to support expenditure submissions for reimbursement shall be provided in accordance with generally accepted accounting principles, including but not limited to timesheets, purchase documents, receipts and pay reconciliation documentation.

d. Invoices submitted by Cardinal Health to Customer pursuant to this Agreement shall be paid by Customer in accordance with the California Prompt Payment Act codified in Title 1, Division 3.6, Part 3, Chapter 4.5, sections 927 through 927.13 of the Government Code.

### **3.03 Dispute Resolution**

In the event Customer disputes a portion of an invoice, Customer shall provide Cardinal Health the following information within seven (7) days of invoice date: (1) invoice number, (2) amount disputed, and (3) specific details as to the nature of the dispute. The Parties shall use best efforts to resolve any disputes within thirty (30) calendar days from the date Customer provides Cardinal Health with information regarding the invoice dispute as set forth herein. Any credit due to Customer or additional changes resulting from the dispute resolution shall appear as a line item on Customer's next monthly invoice. Each Party shall appoint a representative to review invoice detail monthly and meet as needed to reconcile.

## **ARTICLE IV TERM AND TERMINATION**

**4.01 Term of Agreement** The term (the "Initial Term") of this Agreement shall begin upon execution of the Agreement by both parties ("Effective Date"), through June 30, 2020 unless subject to earlier termination as set forth below. Thereafter, the Agreement shall be renewed on a month-to-month basis for no greater than (6) successive months upon the same terms and conditions contained herein unless either Party notifies the other in writing no later than thirty (30) days prior to the Termination Date (defined below) of its intent not to renew. The "Termination Date" shall occur upon the expiration of the Initial Term of this Agreement or any extension, or the date on which this Agreement expires pursuant to the exercise by either Party of its termination rights.

**4.01. Default** Either party may affect an early termination of this Agreement upon the occurrence of a material breach by the other party. The non-breaching party must give written notice to the breaching party of the nature and occurrence of such breach. If (i) the breach is not cured by the expiration of sixty (60) days from the date of such notice, or (ii) the breaching party has not made reasonable efforts to effect the cure within such sixty (60) day period, or (iii) the breach cannot reasonably be cured within the sixty (60) day period, then the non-breaching party may, in addition to any and all other rights or remedies it may have, provide written notice to the breaching party that this Agreement will be terminated immediately following the expiration of such sixty (60) day period. Notwithstanding the foregoing, in the event of a payment default that is not resolved through the Dispute Resolution procedures set forth above, Cardinal Health may terminate this Agreement upon ten (10) days' prior written notice.

### **4.02. Termination**

#### **a. Effect of Termination**

- i. Termination shall not affect any liability or obligation of either Party accrued prior to termination.

#### **b. Customer's Duties Upon Notice of Termination**

- i. If applicable, initiate the processes of State Board of Pharmacy notification and re-licensure, including, but not limited to federal and state licenses, as applicable under the laws of the state in which Customer is located. If for any reason any license remains in Cardinal Health's name after termination of this Agreement, Customer shall pay a monthly fee of fifteen thousand dollars (\$15,000) for each month until all licenses



have been established in Customer's name This Section 4.03 (b) (i) shall survive termination of this Agreement.

- ii. Should a Cardinal Health employee or agent continue to work at or provide services to Customer following termination of this Agreement, Customer shall pay Cardinal Health twenty percent (20%) of the employee's or agent's annual base salary in effect at the time unless the Parties arranged otherwise. This shall not apply to any Cardinal Health employee who was previously employed by Customer.
- iii. Upon termination of this Agreement, all Customer specific manuals, policies and procedures utilized in the Pharmacy, and patient records necessary to operate the Pharmacy shall remain in the Pharmacy sufficient to meet the EOP for continuity of patient care as required by TJC. To the maximal extent allowed under California law, Customer agrees to provide Cardinal Health access to or copies of such documents reasonably requested by Cardinal Health to the extent necessary to handle claims brought after termination, subject to execution of appropriate confidentiality agreement.

c. **Physical Inventory.** Upon termination of this Agreement, a physical inventory count of all Pharmacy controlled substances shall be performed according to the applicable federal and state laws and regulations and such records necessary to effect transfer of responsibility for controlled substances to Customer shall be completed.

#### **ARTICLE V FEMA PROVISIONS**

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

5.02. **Compliance with Federal Law, Regulations, and Executive Orders** This is an acknowledgement that the Federal Emergency Management Agency (FEMA) financial assistance will be used to fund all or a portion of the Agreement only. Cardinal Health will comply with all federal law, regulations, executive orders, FEMA policies, procedures, and directives.

5.03. **No Obligation by Federal Government** The Federal Government is not a party to this Agreement and is not subject to any obligations or liabilities to the non-Federal entity, Agency, or any other party pertaining to any matter resulting from the Agreement.

5.04. **Program Fraud and False or Fraudulent Statements or Related Acts** Cardinal Health acknowledges the 31 U.S.C. Chapter 38 (Administrative Remedies for False Claims and Statements) applies to Cardinal Health's action pertaining to this Agreement.

5.05. **Clean Air Act** Cardinal Health agrees to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act, as amended, 42 U.S.C. § 7401 et seq. Cardinal Health agrees to report each violation to the Customer and understands and agrees that Customer will, in turn, report each violation as required to assure notification to the Federal Emergency Management Agency, and the appropriate Environmental Protection Agency Regional Office. Cardinal Health agrees to include these requirements in each subcontract exceeding \$150,000 financed in whole or in part with Federal assistance provided by FEMA.

5.06. **Federal Water Pollution Control Act** Cardinal Health agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Federal Water Pollution Control Act, as amended, 33 U.S.C. 1251 et seq. Cardinal Health agrees to report each violation to the Customer and understands and agrees that the Customer will, in turn, report each violation as required to assure notification to the Federal Emergency Management Agency, and the appropriate Environmental Protection Agency Regional Office. Cardinal Health agrees to include these requirements in each subcontract exceeding \$150,000 financed in whole or in part with Federal assistance provided by FEMA.

5.07. **Debarment and Suspension** This Agreement is a covered transaction for purposes of 2 C.F.R. pt. 180 and 2 C.F.R. pt. 3000. As such, Cardinal Health is required to verify that none of Cardinal Health's principals (defined at 2 C.F.R. § 180.995) or its affiliates (defined at 2 C.F.R. § 180.905) are excluded (defined at 2 C.F.R. § 180.940) or disqualified (defined at 2 C.F.R. § 180.935). Cardinal Health must comply with 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C, and must include a requirement to comply with these regulations in any lower tier covered transaction it enters into. This certification is a material representation of fact relied upon by the Customer. If it is later determined that Cardinal Health did not comply with 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C, in addition to remedies available to the Customer, the Federal Government may pursue available remedies, including but not limited to suspension and/or debarment.

5.08. **Byrd Anti-Lobbying Amendment, 31 U.S.C. § 1352 (as amended)** The contractor who apply or bid for an award of \$100,000 or more shall file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, officer or employee of Congress, or an employee of a Member of Congress in connection with obtaining any Federal contract, grant, or any other award covered by 31 U.S.C. § 1352. Each tier shall also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the recipient who in turn will forward the certification(s) to the awarding agency. Enclosed as **Exhibit B** is a copy of the Certification Regarding Lobbying, 44 C.F.R. PART 18, that will be signed and submitted by Agency at the execution of this Agreement.

## ARTICLE VI GENERAL PROVISIONS

6.01 **Confidentiality** Cardinal Health's pricing, business plans, processes and strategies all constitute "Confidential Information" of Cardinal Health subject to any exclusion under California law. The Parties shall not disclose or use any Confidential Information for any purpose other than as set forth herein. The Parties shall protect the Confidential Information in the same manner that they protect the confidentiality of their own proprietary and confidential information of like kind, but in no event shall they exercise less than reasonable care in protecting such Confidential Information. If either Party is compelled by law to disclose any Confidential Information, it shall provide the other Party with prior notice of such compelled disclosure and reasonable assistance to contest the disclosure. If either Party discloses or uses (or threatens to disclose or use) any Confidential Information of the other Party in breach of this Section, the aggrieved Party shall have the right, in addition to any other remedies available to it, to seek injunctive relief to enjoin such acts, it being specifically acknowledged by the Parties that any other available remedies are inadequate. This Section 5.01 shall survive the termination or expiration of the Agreement for a period of three (3) years. Notwithstanding the foregoing, any obligations of confidentiality and non-use governing Protected Health Information (as defined by HIPAA) that are included in a Business Associate Agreement in effect between the parties shall continue in effect in accordance with the terms of such Agreement and as required by applicable law.

The obligations created by this Section herein shall not apply to particular Confidential Information if the Party in receipt of the Confidential Information ("Recipient") can reasonably demonstrate such Confidential Information:

- a. is in the public domain at the time of the disclosure of Confidential Information by disclosing Party to Recipient;
- b. becomes publicly available subsequent to disclosure of Confidential Information by disclosing Party without Recipient's breach of any obligations owed the disclosing Party;
- c. became known by Recipient at any time from a source other than the disclosing Party and other than by breach of an obligation of confidentiality owed to the disclosing Party;
- d. was otherwise known by Recipient prior to disclosure of Confidential Information by disclosing Party to Recipient; or
- e. was independently developed by Recipient without reference to, exposure to, use of, or disclosure of any Confidential Information.

**6.02 Insurance** Without limiting any other obligation or liability under this Agreement, each Party agrees that upon execution of this Agreement and through its entire effective period, each Party shall at its own cost and expense, to obtain and maintain insurance coverage with limits and conditions not less than those specified below:

- a. Commercial General Liability insurance with a per occurrence limit of not less than two million dollars (\$2,000,000).
- b. Professional Liability insurance with a limit of not less than five million dollars (\$5,000,000).
- c. Workers' Compensation and Employer's Liability insurance with statutory limits for Workers' Compensation and Employer's Liability insurance limits of not less than one million dollars (\$1,000,000). Each Party shall waive subrogation rights against the other.

The Parties acknowledge that either Party may be self-insured for any or all of the coverages and types of losses required in this Section. For the above described insurance policies will be issued by insurance carriers with an A.M. Best Rating of at least A-VII. Upon execution of this Agreement and upon renewal of the required insurance policies, if not self-insured each Party agrees to provide evidence of the insurance required in this Agreement. In the event that any of the above described insurance policies are written on a claims made basis, then such policy(ies) shall be maintained during the entire period of this Agreement and for a period of not less than three (3) years following the termination or expiration of this Agreement.

Cardinal Health shall ensure that its agents and non-employee staff providing services at the Customer maintain and provide evidence of the same insurance that each is required to maintain as described in this Section.

**6.03 Discounts** Any rebates and price reductions provided in this Agreement may constitute a "discount or other reduction in price," as defined under the Medicare/ Medicaid Anti-Kickback Statute, on products and services purchased from Cardinal Health. Customer shall comply with any and all requirements imposed on buyers, respectively, under 42 U.S.C. § 1320a-7b(b)(3)(A) and the "safe harbor" regulations regarding discounts or other reductions in price set forth in 42 C.F.R. § 1001.952(h). Customer may be obligated to accurately report, under state or federal programs which provide cost or charge based reimbursement, the net cost actually paid by Customer.

**6.04 Access to Records** For a period of four (4) years after Cardinal Health has performed the Agreement, Cardinal Health shall make available, upon written request of the Secretary of the Department of Health and Human Services ("Secretary"), or upon request of the Comptroller General of the United States ("Comptroller"), or any of their duly authorized representatives (collectively, the "Requesting Party"), the Agreement and any books, documents, and records necessary to certify the nature and extent of the costs paid by Customer to Cardinal Health pursuant to the Product Agreement ("Access"). If Cardinal Health pays a subcontractor more than \$10,000 over a twelve (12) month period to perform the Agreement, then Cardinal Health shall obligate the subcontractor to permit Access to the Requesting Party.

**6.05 Press Release or Public Announcements** Neither Party will make any press release regarding this Agreement or the transactions contemplated hereby without the other Party's express prior written consent,

except as required under applicable law or by any governmental agency, in which case the Party required to make the press release shall use commercially reasonable efforts to obtain the approval of the other Party as to the form, nature and extent of the press release prior to issuing the press release.

**6.06 Exclusion of Consequential Damages** NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY FOR INCIDENTAL, CONSEQUENTIAL OR SPECIAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOSS OF BUSINESS OR PROFITS.

**6.07 Data** All data submitted by Customer to Cardinal Health pursuant to this Agreement ("Customer Data") remains the sole property of Customer. Customer grants to Cardinal Health a non-exclusive, perpetual, royalty-free license to use, copy, store, modify and display the Customer Data for any lawful purpose, including without limitation, providing the service, creating reports and statistical analyses about the service such as usage or authorized user traffic patterns, and making such data available in aggregate form to third parties, provided that such information does not include Customer's name or personally identifying information. If Customer Data contains Protected Health Information as defined by 45 C.F.R. §164.501, then Cardinal Health shall de-identify that Customer Data pursuant to 45 C.F.R. § 164.514 prior to using or disclosing that Customer Data.

**6.08 Immunity from Liability** Customer represents that California Government Code §§ 8659 and 8567(b), as well as California Civil Code § 1714.5(b), apply to the Agreement which provides, in pertinent part, that health workers the State of California obtains through its agencies, including Customer, shall be entitled to full statutory immunity from general liability in this current state of emergency.

**6.09 Force Majeure** If a Party is reasonably prevented from performing an obligation of this Agreement because of fire, flood, wind, earthquake, explosion or other disaster, acts of military authorities, acts of civil authorities unrelated to any violation of law by the Party, war, riot, insurrection, act of terrorism or other cause beyond the Party's reasonable control (collectively, a "Force Majeure Event"), then that Party shall not be in breach of this Agreement during the period that the Party is prevented from performing the obligation because of the Force Majeure Event provided that the Party (i) promptly delivers notice to the other Party identifying the Force Majeure Event and (ii) exercises reasonable commercial efforts to resume performance as soon as is reasonably possible.

**6.10 Business Associate Obligations.** The Parties agree to be bound by the terms of the business associate agreement set forth in Exhibit C as it relates to the provisions set forth herein to protect confidential patient information under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Privacy and Security Rules, 45 C.F.R. parts 160, 162 and 164 and the Health Information Technology for Economic and Clinical Health Act, included in Division A, Title XIII, Subtitle D of The American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (February 17, 2009), and any regulations or agency guidance issued pursuant thereto ("HITECH").

**6.11 Assignment** Neither Party may assign any rights or obligations under the Agreement without the other Party's prior written consent, which shall not be unreasonably withheld, provided that either Party may with notice assign all of such Party's rights and obligations under the Agreement without the other Party's consent: (i) to an affiliate; or (ii) incident to the transfer of all or substantially all of such Party's business assets.

**6.12 Notices** Any notice from one Party to the other Party shall be in writing and shall be deemed to be given: (i) upon delivery if by hand or by overnight courier; or (ii) three days after mailing, if by certified or registered mail to the receiving Party's Notice Address below. Either Party may change its Notice Address upon delivery of notice to the other Party.

Cardinal Health Pharmacy Services, LLC  
Attn: VP, Managed Services  
13651 Dublin Ct.,  
Stafford, Texas 77477

California Department of Public Health  
Attn: Jen Hill



## Pharmacy Agreement

1616 Capitol Avenue, MS 3202  
Sacramento, California 95814  
Email: [Jennifer.Hill3@cdph.ca.gov](mailto:Jennifer.Hill3@cdph.ca.gov)

**6.13 Severability; Non-Waiver** If a court or other body of competent jurisdiction declares any term of the Agreement invalid or unenforceable, then the remaining terms shall continue in full force and effect. No right created by the Agreement shall be deemed waived unless specifically and expressly waived in a writing signed by the Party possessing the right.

**6.14 Governing Law** The Agreement shall be governed by the laws of the state identified in Customer's Notice Address above, without regard to that state's conflicts of law provisions.


**6.15 Independent Contractor** The Parties expressly acknowledge and agree that Cardinal Health is neither the employer nor joint employer of any of the individuals paid as employees of Customer and that Customer is neither the employer nor joint employer of any of the individuals paid as employees of Cardinal Health.

**6.16 Entire Agreement; Amendment** The Agreement constitutes the entire agreement and understanding of the Parties regarding the subject matter of the Agreement and supersedes all prior written and oral agreements, proposals, and understandings between the Parties regarding the subject matter of the Agreement. No changes to the Agreement shall be effective unless signed by each Party.

**6.17 Agreement Signatures** This Agreement may be executed in one or more counterparts, each of which shall constitute an original, but all of which together shall constitute one instrument. Signatures to this Agreement may be delivered by facsimile, by electronic mail (e.g., a ".pdf" file) or by any other electronic means that is intended to preserve the original appearance of the document, and such delivery will have the same effect as the delivery of the paper document bearing the actual, handwritten signatures.

**Each person signing this Agreement represents that he/she intends to and has the authority to bind his/her Party to this Agreement.**

CALIFORNIA DEPARTMENT OF PUBLIC HEALTH

By: 

Print: Timothy Bow

Title: Procurement Officer, Emergency Operations

Date Signed: 4/14/2020

CARDINAL HEALTH PHARMACY SERVICES, LLC

By:   
Michael D. Brown (Apr 14, 2020)

Print: Michael D. Brown

Title: V.P. Managed Services

Date Signed: Apr 14, 2020

Last Modified on 4/10/2020

**EXHIBIT A**  
**REMOTE PHARMACY SERVICES**

**ARTICLE I**  
**DEFINITIONS & DUTIES**

**1.01** Definitions

- a. "Remote Pharmacy Services" or "Service(s)": Cardinal Health shall provide Customer its service of remote entry of physician medication orders.
- b. "Order Lines": Individual medication orders entered, discontinued, or modified by Cardinal Health.
- c. "Order Entry Variance": Includes, but is not limited to, a Medication Error (as defined below) or a medication entry entered by Cardinal Health that varies from the standard procedure according to Customer's policy and procedures.

**1.02** Drugs Administered to Patients Customer affirms that drugs administered to the Customer's patients shall only be pursuant to lawful order therefore.

**1.03** Customer Duties upon Execution of Agreement To assist in preventing delays by Cardinal Health in starting Services with Customer and prior to being able to go-live with the remote services Customer shall:

- a. Complete implementation forms provided by Cardinal Health;
- b. Establish and complete connectivity with access and testing;
- c. Provide software licenses and media as may be necessary for Cardinal Health to remotely access Customer's system and perform required pharmacy functions; and
- d. Provide login (access) codes for Cardinal Health pharmacists and/or technicians.

**1.04** Customer Duties After Start of Service Customer agrees to provide the following to Cardinal Health, as may be necessary, on an on-going basis once Services have begun:

- a. New login (access) codes that are requested by Cardinal Health are to be provided within three (3) business days of such request;
- b. Best efforts to meet connectivity and system speed standards consistent with Customer's on-site operations;
- c. Best efforts to standardize Customer's order entry process and policies and procedures; and
- d. Complete and fax Order Entry Variance forms.
- e. Notification that there are orders for processing. This notification may be by electronic transmission of order notifications through Cardinal Health's Medication Order Management System software, phone call or via fax to the Cardinal Health pharmacy service team.

**1.05** Employee Confidentiality Cardinal Health will not provide employee-level confidential information, including but not limited to, Social Security Number ("SSN") and/or Date of Birth ("DOB") for reasons of assigning access codes to Customer's pharmacy computer system or for any other reason.

**1.06** Elements of Performance Pursuant to the leadership standards by the applicable accrediting agencies in effect during the term of this Agreement, the Parties agree to monitor "Medication Errors" as a metric for the quality of Services provided pursuant to this Agreement. For purposes of this Agreement, "Medication Errors" shall mean any preventable event that may cause or lead to inappropriate medication use or patient harm occurring as a direct result of Cardinal Health's action or inaction during the Hours of Service, as set forth below.

- a. Standard of Performance It is Customer's expectation that the Order Lines processed by Cardinal Health during the Hours of Service shall have a Medication Error rate of one-half percent (0.5%) or less.



- b. Tracking Cardinal Health shall provide Customer a monthly report of Order Entry Variances and/or Medication Errors as tracked by Cardinal Health's Medication Order Management System. It shall remain the responsibility of Customer's quality director (or designee) to review such report with Customer's leadership and quality committee as applicable.
- c. Termination In such event that Cardinal Health's Medication Error rate exceeds the Standard of Performance, set forth above, for a given three (3) month period, Customer shall notify Cardinal Health of such deficiency and allow Cardinal Health an opportunity to improve its performance. Should Cardinal Health's Medication Error rate exceed the Standard of Performance for a subsequent three (3) month period, Customer shall have the right to terminate the Agreement upon thirty (30) days' written notice to Cardinal Health.

## ARTICLE II REMOTE PHARMACY SERVICES

### 2.01 Remote Pharmacy Services Cardinal Health's Remote Pharmacy Services include:

- a. Offsite pharmacist review and verification of all medication orders entered into the ACF's electronic health information system. Cardinal Health staff shall review and enter all medication Order Lines into Customer's pharmacy information system with an average turnaround time of sixty (60) minutes for routine Order Lines, and an average turnaround time of fifteen (15) minutes for stat Order Lines;
- b. Cardinal Health staff shall review and enter all medication Order Lines into Customer's pharmacy information system with a targeted Order Entry Variance rate of less than one-half percent (0.5%);
- c. Cardinal Health pharmacists shall intervene on incomplete or questionable orders with appropriate Customer medical staff and shall make best efforts to resolve interventions during the shift;
- d. Cardinal Health pharmacists shall be available by telephone to respond and/or provide information and clinical support to Customer's staff;
- e. The PIC/DOP and Customer designee shall have access to Cardinal Health's web-based client portal from which reports detailing Cardinal Health's Order Line processing activities may be printed;
- f. Cardinal Health shall record and maintain daily Order Line volume to support Cardinal Health's Order Line processing activities;
- g. Cardinal Health shall provide reports measuring operational, financial and clinical progress towards goals in its customary form. In addition, Cardinal Health shall provide reports in a manner sufficient to meet the Elements of Performance ("EOP") for contracted services as required by TJC. Standardized tracking and reporting of productivity, clinical and quality metrics shall be provided to Customer on a daily basis with clinical consultations documented and reported to Pharmacy on a monthly basis.
- h. Cardinal Health pharmacist may provide video verification services as needed to verify technicians retrieval of the correct medication from the Pharmacy. Customer agrees to provide a high definition camera in order for Cardinal Health to provide this service.
- i. Cardinal Health shall provide training to Customer's staff on remote processes, application and software systems specific to facilitate remote services at the ACF.
- j. Cardinal Health shall provide IT support 24 hours a day, 7 days a week during the time period of the agreement, to ensure availability of Service and secure connection to the ACF pharmacy's health information system. Cardinal Health shall not be responsible for IT issues relating to Customer's systems.
- k. An implementation pharmacist to complete an order processing assessment and create order verification policies and procedures for the ACF Pharmacy;
- l. Ongoing delivery of remote pharmacy coverage at the ACF Pharmacy

- 2.02 Hours of Service Cardinal Health shall provide Remote Pharmacy Services to the ACF 24 hours a day, 7 days a week, and Customer shall provide reasonable advanced notice to Cardinal Health RPS Center Director of any change in dates, times and hours of service.
- 2.03 Start-Up Fee The Start-up Fee set forth in Section 3.01 of the Pharmacy Agreement includes the startup costs associated with the evaluation of Customer processes by Cardinal Health staff, training of Cardinal Health staff on Customer procedures, as well as computer-related expenses to integrate Cardinal Health Services into Customer's system. The Start-Up Fee shall be included on the first Service invoice to Customer.
- a. Should Customer require additional equipment or software licenses to enable integration into Cardinal Health's Services, the costs for such equipment or software license shall be in addition to the Start-Up Fee and shall appear as a line item charge on the next monthly Service invoice to Customer.
  - c. Cancellation Prior to Start of Service
    - i. Should Customer terminate this Agreement prior to commencement of Service and Cardinal Health has not performed the evaluation as noted above, Customer agrees to pay Cardinal Health a Cancellation Fee equal to fifty percent (50%) of the Start-Up Fee.
    - ii. If Cardinal Health has performed the evaluation noted above and Customer terminates this Agreement prior to commencement of Service, it shall remain a responsibility of Customer to pay Cardinal Health the full Start-Up Fee.
- 2.04 Order Transmission Process Change If Customer changes its process by which medication order sheets are transmitted to Cardinal Health, whether from "fax transmission" to "digital scan technology" or the reverse, or by way of another method altogether, either Party shall have the option to renegotiate the financial terms of this Agreement.





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

The undersigned certifies, to the best of his or her knowledge and belief, that:

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

Date Apr 14, 2020

**EXHIBIT C**  
**BUSINESS ASSOCIATE AGREEMENT**

**I. Recitals**

- A. The underlying contract (Agreement), to which this HIPAA Business Associate Addendum is attached to and made a part of, has been determined to constitute a business associate relationship under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (the HITECH Act), 42 U.S.C. section 17921 et seq., and their implementing privacy and security regulations at 45 CFR Parts 160 and 164 ("the HIPAA regulations").
- B. The Department of Public Health ("CDPH") wishes to disclose to Business Associate certain information pursuant to the terms of the Agreement, some of which may constitute Protected Health Information ("PHI"), including protected health information in electronic media ("ePHI"), under federal law, and personal information ("PI") under state law.
- C. As set forth in the Agreement, Contractor, here and after, is the Business Associate of CDPH acting on CDPH' behalf and provides services, arranges, performs or assists in the performance of functions or activities on behalf of CDPH and creates, receives, maintains, transmits, uses or discloses PHI and PI. CDPH and Business Associate are each a party to the Agreement and are collectively referred to as the "parties."
- D. The purpose of this Addendum is to protect the privacy and security of the PHI and PI that may be created, received, maintained, transmitted, used or disclosed pursuant to the Agreement, and to comply with certain standards and requirements of HIPAA, the HITECH Act and the HIPAA regulations, including, but not limited to, the requirement that CDPH must enter into a contract containing specific requirements with Contractor prior to the disclosure of PHI to Contractor, as set forth in 45 CFR Parts 160 and 164 and the HITECH Act.
- E. The terms used in this Addendum, but not otherwise defined, shall have the same meanings as those terms have in the HIPAA regulations. Any reference to statutory or regulatory language shall be to such language as in effect or as amended.

**II. Definitions**

- A. Breach shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.
- B. Business Associate shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.
- C. Covered Entity shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.
- D. Electronic Health Record shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C Section 17921 and implementing regulations.
- E. Electronic Protected Health Information (ePHI) means individually identifiable health information transmitted by electronic media or maintained in electronic media, including but not limited to electronic media as set forth under 45 CFR section 160.103.
- F. Individually Identifiable Health Information means health information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer or health care clearinghouse, and relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, that identifies the individual or where there is a

reasonable basis to believe the information can be used to identify the individual, as set forth under 45 CFR section 160.103.

- G. Privacy Rule shall mean the HIPAA Regulation that is found at 45 CFR Parts 160 and 164.
- H. Personal Information shall have the meaning given to such term in California Civil Code sections 1798.3 and 1798.29.
- I. Protected Health Information means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or is transmitted or maintained in any other form or medium, as set forth under 45 CFR section 160.103.
- J. Required by law, as set forth under 45 CFR section 164.103, means a mandate contained in law that compels an entity to make a use or disclosure of PHI that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants, subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information, and a civil or an authorized investigative demand. It also includes Medicare conditions of participation with respect to health care providers participating in the program, and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.
- K. Secretary means the Secretary of the U.S. Department of Health and Human Services ("HHS") or the Secretary's designee.
- L. Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI or PI, or confidential data that is essential to the ongoing operation of the Business Associate's organization and intended for internal use; or interference with system operations in an information system.
- M. Security Rule shall mean the HIPAA regulation that is found at 45 CFR Parts 160 and 164.
- N. Unsecured PHI shall have the meaning given to such term under the HITECH Act, 42 U.S.C. section 17932(h), any guidance issued pursuant to such Act and the HIPAA regulations.

### **III. Terms of Agreement**

#### **A. Permitted Uses and Disclosures of PHI by Business Associate**

**Permitted Uses and Disclosures.** Except as otherwise indicated in this Addendum, Business Associate may use or disclose PHI only to perform functions, activities or services specified in the Agreement, for, or on behalf of CDPH, provided that such use or disclosure would not violate the HIPAA regulations, if done by CDPH. Any such use or disclosure must, to the extent practicable, be limited to the limited data set, as defined in 45 CFR section 164.514(e)(2), or, if needed, to the minimum necessary to accomplish the intended purpose of such use or disclosure, in compliance with the HITECH Act and any guidance issued pursuant to such Act, and the HIPAA regulations.

1. **Specific Use and Disclosure Provisions.** Except as otherwise indicated in this Addendum, Business Associate may:
  - a. **Use and disclose for management and administration.** Use and disclose PHI for the proper management and administration of the Business Associate provided that such disclosures are required by law, or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and will be used or further disclosed only as required by law or for the purpose for which it was disclosed to the person,

and the person notifies the Business Associate of any instances of which it is aware that the confidentiality of the information has been breached.

- b. **Provision of Data Aggregation Services.** Use PHI to provide data aggregation services to CDPH. Data aggregation means the combining of PHI created or received by the Business Associate on behalf of CDPH with PHI received by the Business Associate in its capacity as the Business Associate of another covered entity, to permit data analyses that relate to the health care operations of CDPH.
- c. Business Associate may "de-identify" PHI in accordance with 45 CFR §164.514(b)(2) and use or disclose "de-identified" information in a manner consistent with and permitted by HIPAA.

#### **B. Prohibited Uses and Disclosures**

1. Business Associate shall not disclose PHI about an individual to a health plan for payment or health care operations purposes if the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full and the individual requests such restriction, in accordance with 42 U.S.C. section 17935(a) and 45 CFR section 164.522(a).
2. Business Associate shall not directly or indirectly receive remuneration in exchange for PHI, except with the prior written consent of CDPH and as permitted by 42 U.S.C. section 17935(d)(2).

#### **C. Responsibilities of Business Associate**

Business Associate agrees:

1. **Nondisclosure.** Not to use or disclose Protected Health Information (PHI) other than as permitted or required by the Agreement or as required by law.
2. **Safeguards.** To implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI, including electronic PHI, that it creates, receives, maintains, uses or transmits on behalf of CDPH, in compliance with 45 CFR sections 164.308, 164.310 and 164.312, and to prevent use or disclosure of PHI other than as provided for by the Agreement, Business Associate shall implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of 45 CFR section 164, subpart C, in compliance with 45 CFR section 164.316. Business Associate 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 Business Associate's operations and the nature and scope of its activities, and which incorporates the requirements of section 3, Security, below. Upon written request, Business Associate will provide CDPH with the Table of Contents of its policies.
3. **Security.** To take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:
  - a. Complying with all of the data system security precautions listed in Attachment A, the Business Associate Data Security Requirements;
  - b. Achieving and maintaining compliance with the HIPAA Security Rule (45 CFR Parts 160 and 164), as necessary in conducting operations on behalf of CDPH under the Agreement;
  - c. Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III - Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and

- d. In case of a conflict between any of the security standards contained in any of these enumerated sources of security standards, the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to PHI from unauthorized disclosure. Further, Business Associate must comply with changes to these standards that occur after the effective date of the Agreement.
- e. Business Associate shall designate a Security Officer to oversee its data security program who shall be responsible for carrying out the requirements of this section and for communicating on security matters with CDPH.

**D. Mitigation of Harmful Effects.** To mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate or its subcontractors in violation of the requirements of this Addendum.

**E. Business Associate's Agents and Subcontractors.**

- 1. To enter into written agreements with any agents, including subcontractors and vendors, to whom Business Associate provides PHI or PI received from or created or received by Business Associate on behalf of CDPH, that impose the same restrictions and conditions on such agents, subcontractors and vendors that apply to Business Associate with respect to such PHI and PI under this Addendum, and that comply with all applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations.
- 2. In accordance with 45 CFR section 164.504(e)(1)(ii), upon Business Associate's knowledge of a material breach or violation by its subcontractor of the agreement between Business Associate and the subcontractor, Business Associate shall:
  - a. Provide an opportunity for the subcontractor to cure the breach or end the violation and terminate the agreement if the subcontractor does not cure the breach or end the violation within the time specified by CDPH; or
  - b. Immediately terminate the agreement if the subcontractor has breached a material term of the agreement and cure is not possible.

**F. Availability of Information to CDPH and Individuals.** To provide access and information:

- 1. To provide access as CDPH may require, and in the time and manner designated by CDPH (upon reasonable notice and during Business Associate's normal business hours) to PHI in a Designated Record Set, to CDPH (or, as directed by CDPH), to an Individual, in accordance with 45 CFR section 164.524. Designated Record Set means the group of records maintained for CDPH that includes medical, dental and billing records about individuals; enrollment, payment, claims adjudication, and case or medical management systems maintained for CDPH health plans; or those records used to make decisions about individuals on behalf of CDPH. Business Associate shall use the forms and processes developed by CDPH for this purpose and shall respond to requests for access to records transmitted by CDPH within fifteen (15) calendar days of receipt of the request by producing the records or verifying that there are none.
- 2. If Business Associate maintains an Electronic Health Record with PHI, and an individual requests a copy of such information in an electronic format, Business Associate shall provide such information in an electronic format to enable CDPH to fulfill its obligations under the HITECH Act, including but not limited to, 42 U.S.C. section 17935(e).
- 3. If Business Associate receives data from CDPH that was provided to CDPH by the Social Security Administration, upon request by CDPH, Business Associate shall provide CDPH with a list of all employees, contractors and agents who have access to the Social Security data, including employees, contractors and agents of its subcontractors and agents.

- G. Amendment of PHI.** To make any amendment(s) to PHI that CDPH directs or agrees to pursuant to 45 CFR section 164.526, in the time and manner reasonably designated by CDPH.
- H. Internal Practices.** To make Business Associate's internal practices, books and records relating to the use and disclosure of PHI received from CDPH, or created or received by Business Associate on behalf of CDPH, available to the Secretary of the U.S. Department of Health and Human Services in a time and manner designated by the Secretary, for purposes of determining CDPH's compliance with the HIPAA regulations. If any information needed for this purpose is in the exclusive possession of any other entity or person and the other entity or person fails or refuses to furnish the information to Business Associate, Business Associate shall so certify to CDPH and shall set forth the efforts it made to obtain the information.
- I. Documentation of Disclosures.** To document and make available to CDPH or (at the direction of CDPH) to an Individual such disclosures of PHI, and information related to such disclosures, necessary to respond to a proper request by the subject Individual for an accounting of disclosures of PHI, in accordance with the HITECH Act and its implementing regulations, including but not limited to 45 CFR section 164.528 and 42 U.S.C. section 17935(c). If Business Associate maintains electronic health records for CDPH as of January 1, 2009, Business Associate must provide an accounting of disclosures, including those disclosures for treatment, payment or health care operations, effective with disclosures on or after January 1, 2014. If Business Associate acquires electronic health records for CDPH after January 1, 2009, Business Associate must provide an accounting of disclosures, including those disclosures for treatment, payment or health care operations, effective with disclosures on or after the date the electronic health record is acquired, or on or after January 1, 2011, whichever date is later. The electronic accounting of disclosures shall be for disclosures during the three years prior to the request for an accounting.
- J. Breaches and Security Incidents.** During the term of the Agreement, Business Associate agrees to implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and to take the following steps:
- 1. Notice to CDPH.** (1) To notify CDPH **promptly, without unreasonable delay, by telephone call plus email or fax** upon the discovery of a breach of unsecured PHI or PI in electronic media or in any other media if the PHI or PI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, or upon the discovery of an actual security incident that involves data provided to CDPH by the Social Security Administration. (2) To notify CDPH **within 48 hours by email or fax** of the discovery of any actual security incident, intrusion or unauthorized access, use or disclosure of PHI or PI in violation of the Agreement and this Addendum, or potential loss of confidential data affecting the Agreement. A breach shall be treated as discovered by Business Associate as of the first day on which the breach is confirmed, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of Business Associate.

Any attempted, but unsuccessful Security Incident of which Business Associate becomes aware will be reported to Covered Entity orally or in writing upon the written reasonable request of Covered Entity. If the HIPAA Security Regulations are amended to remove the requirement to report unsuccessful attempts at unauthorized access, the requirement to report such unsuccessful attempts shall no longer apply as of the effective date of that amendment.

Notice shall be provided to the CDPH Program Contract Manager, the CDPH Privacy Officer and the CDPH Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves electronic PHI, notice shall be provided by calling the CDPH ITSD Service Desk. Notice shall be made using the "CDPH Privacy Incident Report" form, including all information known at the time. Business Associate shall use the most current version of this form, which is posted on the CDPH Privacy Office website ([www.CDPH.ca.gov](http://www.CDPH.ca.gov)).

Upon discovery of a breach or actual security incident, intrusion or unauthorized access, use or disclosure of PHI or PI, Business Associate shall take:

- a. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and
  - b. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.
2. **Investigation and Investigation Report.** To promptly, without unreasonable delay, investigate such security incident, breach, or unauthorized access, use or disclosure of PHI or PI. Within three (3) business days of the discovery, Business Associate shall submit an updated "CDPH Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Information Security Officer:
3. **Complete Report.** To provide a complete report of the investigation to the CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Information Security Officer within ten (10) working days of the confirmation of the breach or unauthorized use or disclosure. The report shall be submitted on the "CDPH Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable provisions of HIPAA, the HITECH Act, the HIPAA regulations and/or state law. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If CDPH requests information in addition to that listed on the "CDPH Privacy Incident Report" form, Business Associate shall make reasonable efforts to provide CDPH with such information. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "CDPH Privacy Incident Report" form. CDPH will review and approve the determination of whether a breach occurred and individual notifications are required, and the corrective action plan.
4. **Notification of Individuals.** If the cause of a breach of PHI or PI is attributable to Business Associate or its subcontractors, agents or vendors, Business Associate shall notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal law and shall pay any costs of such notifications, as well as any costs associated with the breach. The notifications shall comply with the requirements set forth in 42 U.S.C. section 17932 and its implementing regulations, including, but not limited to, the requirement that the notifications be made without unreasonable delay and in no event later than 60 calendar days. The CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Information Security Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made.
5. **Responsibility for Reporting of Breaches.** If the cause of a breach of PHI or PI is attributable to Business Associate or its agents, subcontractors or vendors, Business Associate is responsible for all required reporting of the breach as specified in 42 U.S.C. section 17932 and its implementing regulations, including notification to media outlets and to the Secretary. If a breach of unsecured PHI involves more than 500 residents of the State of California or its jurisdiction, Business Associate shall notify the Secretary of the breach promptly upon discovery of the breach. If Business Associate has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to CDPH in addition to Business Associate, Business Associate shall notify CDPH, and CDPH and Business Associate may take appropriate action to prevent duplicate reporting. The breach reporting requirements of this paragraph are in addition to the reporting requirements set forth in subsection 1, above.
6. **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 giving written notice to the Contractor. Said changes shall not require an amendment to this Addendum or the Agreement to which it is incorporated.

<b>CDPH Contract Manager</b>	<b>CDPH Privacy Officer</b>	<b>CDPH Information Security Officer</b>
See the Scope of Work exhibit for Program Contract Manager information	Privacy Officer Privacy Office, c/o Office of Legal Services California Department of Public Health 1415 L Street, 5 <sup>th</sup> Floor Sacramento, CA 95814  Email: <a href="mailto:privacy@cdph.ca.gov">privacy@cdph.ca.gov</a> Telephone: (877) 421-9634	Chief Information Security Officer Information Security Office California Department of Public Health P.O. Box 997413, MS 6302 Sacramento, CA 95899-7413  Email: <a href="mailto:cdphiso@cdph.ca.gov">cdphiso@cdph.ca.gov</a> Telephone: IT Service Desk (916) 440-7000 or (800) 579-0874

**K. Termination of Agreement.** In accordance with Section 13404(b) of the HITECH Act and to the extent required by the HIPAA regulations, if Business Associate knows of a material breach or violation by CDPH of this Addendum, it shall take the following steps:

1. Provide an opportunity for CDPH to cure the breach or end the violation and terminate the Agreement if CDPH does not cure the breach or end the violation within the reasonable time specified by Business Associate; or
2. Immediately terminate the Agreement if CDPH has breached a material term of the Addendum and cure is not possible.

**L. Due Diligence.** Business Associate shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this Addendum and is in compliance with applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations, and that its agents, subcontractors and vendors are in compliance with their obligations as required by this Addendum.

**M. Sanctions and/or Penalties.** Business Associate understands that a failure to comply with the provisions of HIPAA, the HITECH Act and the HIPAA regulations that are applicable to Business Associate may result in the imposition of sanctions and/or penalties on Business Associate under HIPAA, the HITECH Act and the HIPAA regulations.

#### **IV. Obligations of CDPH**

CDPH agrees to:

- A. Notice of Privacy Practices.** Provide Business Associate with the Notice of Privacy Practices that CDPH produces in accordance with 45 CFR section 164.520, as well as any changes to such notice.
- B. Permission by Individuals for Use and Disclosure of PHI.** Provide the Business Associate with any changes in, or revocation of, permission by an individual to use or disclose PHI, if such changes affect the Business Associate's permitted or required uses and disclosures.
- C. Notification of Restrictions.** Notify the Business Associate of any restriction to the use or disclosure of PHI that CDPH has agreed to in accordance with 45 CFR section 164.522, to the extent that such restriction may affect the Business Associate's use or disclosure of PHI.
- D. Requests Conflicting with HIPAA Rules.** Not request the Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA regulations if done by CDPH.



## V. Audits, Inspection and Enforcement

- A. From time to time, Business Associate agrees to make its security policies Table of Contents or redacted copies of its policies and procedures available to CDPH upon written request to monitor Business Associate's compliance with the Agreement and this Addendum. Business Associate shall promptly remedy any violation of any provision of this Addendum and shall certify the same to the CDPH Privacy Officer in writing. The fact that CDPH inspects, or fails to inspect, or has the right to inspect, Business Associate's policies and procedures does not relieve Business Associate of its responsibility to comply with this Addendum, nor does CDPH's:
1. Failure to detect or
  2. Detection, but failure to notify Business Associate or require Business Associate's remediation of any unsatisfactory practices constitute acceptance of such practice or a waiver of CDPH' enforcement rights under the Agreement and this Addendum.
- B. If Business Associate is the subject of an audit, compliance review, or complaint investigation by the Secretary or the Office of Civil Rights, U.S. Department of Health and Human Services, that is related to the performance of its obligations pursuant to this HIPAA Business Associate Addendum, Business Associate shall notify CDPH and provide CDPH with a copy of any PHI or PI that Business Associate provides to the Secretary or the Office of Civil Rights concurrently with providing such PHI or PI to the Secretary. Business Associate is responsible for any civil penalties assessed due to an audit or investigation of Business Associate, in accordance with 42 U.S.C. section 17934(c).

## VI. Termination

- A. **Term.** The Term of this Addendum shall commence as of the effective date of this Addendum and shall extend beyond the termination of the Agreement and shall terminate when all the PHI provided by CDPH to Business Associate, or created or received by Business Associate on behalf of CDPH, is destroyed or returned to CDPH, in accordance with 45 CFR 164.504(e)(2)(ii)(I).
- B. **Termination for Cause.** In accordance with 45 CFR section 164.504(e)(1)(ii), upon CDPH' knowledge of a material breach or violation of this Addendum by Business Associate, CDPH shall:
1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate the Agreement if Business Associate does not cure the breach or end the violation within the reasonable time specified by CDPH; or
  2. Immediately terminate the Agreement if Business Associate has breached a material term of this Addendum and cure is not possible.
- C. **Judicial or Administrative Proceedings.** Business Associate will notify CDPH if it is named as a defendant in a criminal proceeding for a violation of HIPAA. CDPH may terminate the Agreement if Business Associate is found guilty of a criminal violation of HIPAA. CDPH may terminate the Agreement if a finding or stipulation that the Business Associate has violated any standard or requirement of HIPAA, or other security or privacy laws is made in any administrative or civil proceeding in which the Business Associate is a party or has been joined.
- D. **Effect of Termination.** Upon termination or expiration of the Agreement for any reason, Business Associate shall return or destroy all PHI received from CDPH (or created or received by Business Associate on behalf of CDPH) that Business Associate still maintains in any form, and shall retain no copies of such PHI. If return or destruction is not feasible, Business Associate shall notify CDPH of the conditions that make the return or destruction infeasible, and CDPH and Business Associate shall determine the terms and conditions under which Business Associate may retain the PHI. Business Associate shall continue to extend the protections of this Addendum to such PHI, and shall limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate.

## VII. Miscellaneous Provisions

- A. *Disclaimer.*** CDPH makes no warranty or representation that compliance by Business Associate with this Addendum, HIPAA or the HIPAA regulations will be adequate or satisfactory for Business Associate's own purposes or that any information in Business Associate's possession or control, or transmitted or received by Business Associate, is or will be secure from unauthorized use or disclosure. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI.
- B. *Amendment.*** The parties acknowledge that federal and state laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Addendum may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, the HIPAA regulations and other applicable laws relating to the security or privacy of PHI. Upon CDPH' request, Business Associate agrees to promptly enter into negotiations with CDPH concerning an amendment to this Addendum embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, the HIPAA regulations or other applicable laws. CDPH may terminate the Agreement upon thirty (30) days written notice in the event:
1. Business Associate does not promptly enter into negotiations to amend this Addendum when requested by CDPH pursuant to this Section; or
  2. Business Associate does not enter into an amendment providing assurances regarding the safeguarding of PHI that the parties mutually deem sufficient to satisfy the standards and requirements of HIPAA and the HIPAA regulations.
- C. *Assistance in Litigation or Administrative Proceedings.*** Business Associate shall make itself and any subcontractors, employees or agents assisting Business Associate in the performance of its obligations under the Agreement, available to CDPH at no cost to CDPH to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CDPH, its directors, officers or employees based upon claimed violation of HIPAA, the HIPAA regulations or other laws relating to security and privacy, which involves inactions or actions by the Business Associate, except where Business Associate or its subcontractor, employee or agent is a named adverse party.
- D. *No Third-Party Beneficiaries.*** Nothing express or implied in the terms and conditions of this Addendum is intended to confer, nor shall anything herein confer, upon any person other than CDPH or Business Associate and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.
- E. *Interpretation.*** The terms and conditions in this Addendum shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, the HIPAA regulations and applicable state laws. The parties agree that any ambiguity in the terms and conditions of this Addendum shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act and the HIPAA regulations.
- F. *Regulatory References.*** A reference in the terms and conditions of this Addendum to a section in the HIPAA regulations means the section as in effect or as amended.
- G. *Survival.*** The respective rights and obligations of Business Associate under Section VI.D of this Addendum shall survive the termination or expiration of the Agreement.
- H. *No Waiver of Obligations.*** No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.

**Attachment A**

**Business Associate Data Security Requirements**

**I. Personnel Controls**

- A. Employee Training.** All workforce members who assist in the performance of functions or activities on behalf of CDPH, or access or disclose CDPH PHI or PI must complete information privacy and security training, at least annually, at Business Associate's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following contract termination.
- B. Employee Discipline.** Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.
- C. Confidentiality Statement.** All persons that will be working with CDPH PHI or PI must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to CDPH PHI or PI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for CDPH inspection for a period of six (6) years following contract termination. The confidentiality statement must be provided to Business Associate by CDPH upon start of the Agreement and annually thereafter.
- D. Workforce Member Assessment.** Before a member of the Contractor's workforce may access CDPH PCI, Contractor must ensure that all workforce members that will have access to CDPH PCI have been assessed to assure that there is no indication that the workforce member may present a risk to the security or integrity of CDPH PCI. Contractor shall retain each workforce member's assessment documentation, whether in physical or electronic format, for a period of three (3) years following contract termination.

**II. Technical Security Controls**

- A. Workstation/Laptop encryption.** All workstations and laptops that process and/or store CDPH PHI or PI must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the CDPH Information Security Office.
- B. Server Security.** Servers containing unencrypted CDPH PHI or PI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.
- C. Minimum Necessary.** Only the minimum necessary amount of CDPH PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.
- D. Removable media devices.** All electronic files that contain CDPH PHI or PI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, Blackberry, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.
- E. Antivirus software.** All workstations, laptops and other systems that process and/or store CDPH PHI or PI must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

- F. Patch Management.** All workstations, laptops and other systems that process and/or store CDPH PHI or PI must have critical 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 except in situations when assessed risk is considered to be too high.
- G. User IDs and Password Controls.** All users must be issued a unique user name for accessing CDPH PHI or PI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within 24 hours. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every 90 days, preferably every 60 days. Passwords must be changed if revealed or compromised. Passwords 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)
- H. Data Destruction.** When no longer needed, all CDPH PHI or PI must be wiped using the Gutmann or US Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission of the CDPH Information Security Office.
- I. System Timeout.** The system providing access to CDPH PHI or PI must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.
- J. Warning Banners.** All systems providing access to CDPH PHI or PI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.
- K. System Logging.** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for CDPH PHI or PI, or which alters CDPH PHI or PI. 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. If CDPH PHI or PI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.
- L. Access Controls.** The system providing access to CDPH PHI or PI must use role based access controls for all user authentications, enforcing the principle of least privilege.
- M. Transmission encryption.** All data transmissions of CDPH PHI or PI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing PHI can be encrypted. This requirement pertains to any type of PHI or PI in motion such as website access, file transfer, and E-Mail.
- N. Intrusion Detection.** All systems involved in accessing, holding, transporting, and protecting CDPH PHI or PI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

### III. Audit Controls

- A. **System Security Review.** All systems processing and/or storing CDPH PHI or PI 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 should include vulnerability scanning tools.
- B. **Log Reviews.** All systems processing and/or storing CDPH PHI or PI must have a routine procedure in place to review system logs for unauthorized access.
- C. **Change Control.** All systems processing and/or storing CDPH PHI or PI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

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

- A. **Emergency Mode Operation Plan.** Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic CDPH PHI or PI 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 the Agreement for more than 24 hours.
- B. **Data Backup Plan.** Contractor must have established documented procedures to backup CDPH PHI to maintain retrievable exact copies of CDPH PHI or PI. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore CDPH PHI or PI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of CDPH data.

#### V. Paper Document Controls

- A. **Supervision of Data.** CDPH PHI or PI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. CDPH PHI or PI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.
- B. **Escorting Visitors.** Visitors to areas where CDPH PHI or PI is contained shall be escorted and CDPH PHI or PI shall be kept out of sight while visitors are in the area.
- C. **Confidential Destruction.** CDPH PHI or PI must be disposed of through confidential means, such as cross cut shredding and pulverizing.
- D. **Removal of Data.** CDPH PHI or PI must not be removed from the premises of the Contractor except with express written permission of CDPH.
- E. **Faxing.** Faxes containing CDPH PHI or PI 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 the fax.
- F. **Mailing.** Mailings of CDPH PHI or PI shall be sealed and secured from damage or inappropriate viewing of PHI or PI to the extent possible. Mailings which include 500 or more individually identifiable records of CDPH PHI or PI 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.






# California Dept of Public Health pharmacy mgmt agmt

Final Audit Report

2020-04-14

Created:	2020-04-14
By:	Robin Popp (robin.popp@cardinalhealth.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAWhlpqEe_RU7dtZ0Wwr2-ebzkwUipUvs3

## "California Dept of Public Health pharmacy mgmt agmt" History

-  Document created by Robin Popp (robin.popp@cardinalhealth.com)  
2020-04-14 - 11:31:25 PM GMT- IP address: 199.230.203.247
  
-  Document emailed to Michael D. Brown (mike.brown@cardinalhealth.com) for signature  
2020-04-14 - 11:34:37 PM GMT
  
-  Email viewed by Michael D. Brown (mike.brown@cardinalhealth.com)  
2020-04-14 - 11:49:26 PM GMT- IP address: 98.195.221.237
  
-  Document e-signed by Michael D. Brown (mike.brown@cardinalhealth.com)  
Signature Date: 2020-04-14 - 11:50:05 PM GMT - Time Source: server- IP address: 98.195.221.237
  
-  Signed document emailed to Robin Popp (robin.popp@cardinalhealth.com),  
christy.cummings@cardinalhealth.com and Michael D. Brown (mike.brown@cardinalhealth.com)  
2020-04-14 - 11:50:05 PM GMT

**Attachment 1**  
**HIPAA Business Associate Addendum**

**I. Recitals**

- A. The underlying contract (Agreement), to which this HIPAA Business Associate Addendum is attached to and made a part of, has been determined to constitute a business associate relationship under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("the HITECH Act"), 42 U.S.C. section 17921 et seq., and their implementing privacy and security regulations at 45 CFR Parts 160 and 164 ("the HIPAA regulations").
- B. The Department of Public Health ("CDPH") wishes to disclose to Business Associate certain information pursuant to the terms of the Agreement, some of which may constitute Protected Health Information ("PHI"), including protected health information in electronic media ("ePHI"), under federal law, and personal information ("PI") under state law.
- C. As set forth in the Agreement, Contractor, here and after, is the Business Associate of CDPH acting on CDPH's behalf and provides services, arranges, performs or assists in the performance of functions or activities on behalf of CDPH and creates, receives, maintains, transmits, uses or discloses PHI and PI. CDPH and Business Associate are each a party to the Agreement and are collectively referred to as the "parties."
- D. The purpose of this Addendum is to protect the privacy and security of the PHI and PI that may be created, received, maintained, transmitted, used or disclosed pursuant to the Agreement, and to comply with certain standards and requirements of HIPAA, the HITECH Act and the HIPAA regulations, including, but not limited to, the requirement that CDPH must enter into a contract containing specific requirements with Contractor prior to the disclosure of PHI to Contractor, as set forth in 45 CFR Parts 160 and 164 and the HITECH Act.
- E. The terms used in this Addendum, but not otherwise defined, shall have the same meanings as those terms have in the HIPAA regulations. Any reference to statutory or regulatory language shall be to such language as in effect or as amended.

**II. Definitions**

- A. Breach shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.
- B. Business Associate shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.
- C. Covered Entity shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.
- D. Electronic Health Record shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C Section 17921 and implementing regulations.
- E. Electronic Protected Health Information (ePHI) means individually identifiable health information transmitted by electronic media or maintained in electronic media, including but not limited to electronic media as set forth under 45 CFR section 160.103.
- F. Individually Identifiable Health Information means health information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer or health care clearinghouse, and relates to the past, present or future physical or mental health or

**Attachment 1**  
**HIPAA Business Associate Addendum**

condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, that identifies the individual or where there is a reasonable basis to believe the information can be used to identify the individual, as set forth under 45 CFR section 160.103.

- G. Privacy Rule shall mean the HIPAA Regulation that is found at 45 CFR Parts 160 and 164.
- H. Personal Information shall have the meaning given to such term in California Civil Code sections 1798.3 and 1798.29.
- I. Protected Health Information means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or is transmitted or maintained in any other form or medium, as set forth under 45 CFR section 160.103.
- J. Required by law, as set forth under 45 CFR section 164.103, means a mandate contained in law that compels an entity to make a use or disclosure of PHI that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants, subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information, and a civil or an authorized investigative demand. It also includes Medicare conditions of participation with respect to health care providers participating in the program, and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.
- K. Secretary means the Secretary of the U.S. Department of Health and Human Services ("HHS") or the Secretary's designee.
- L. Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI or PI, or confidential data that is essential to the ongoing operation of the Business Associate's organization and intended for internal use; or interference with system operations in an information system.
- M. Security Rule shall mean the HIPAA regulation that is found at 45 CFR Parts 160 and 164.
- N. Unsecured PHI shall have the meaning given to such term under the HITECH Act, 42 U.S.C. section 17932(h), any guidance issued pursuant to such Act and the HIPAA regulations.

### **III. Terms of Agreement**

#### **A. Permitted Uses and Disclosures of PHI by Business Associate**

**Permitted Uses and Disclosures.** Except as otherwise indicated in this Addendum, Business Associate may use or disclose PHI only to perform functions, activities or services specified in the Agreement, for, or on behalf of CDPH, provided that such use or disclosure would not violate the HIPAA regulations, if done by CDPH. Any such use or disclosure must, to the extent practicable, be limited to the limited data set, as defined in 45 CFR section 164.514(e)(2), or, if needed, to the minimum necessary to accomplish the intended purpose of such use or disclosure, in compliance with the HITECH Act and any guidance issued pursuant to such Act, and the HIPAA regulations.

1. **Specific Use and Disclosure Provisions.** Except as otherwise indicated in this Addendum, Business Associate may:



**Attachment 1**  
**HIPAA Business Associate Addendum**

- a. **Use and disclose for management and administration.** Use and disclose PHI for the proper management and administration of the Business Associate provided that such disclosures are required by law, or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and will be used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware that the confidentiality of the information has been breached.
- b. **Provision of Data Aggregation Services.** Use PHI to provide data aggregation services to CDPH. Data aggregation means the combining of PHI created or received by the Business Associate on behalf of CDPH with PHI received by the Business Associate in its capacity as the Business Associate of another covered entity, to permit data analyses that relate to the health care operations of CDPH.
- c. Business Associate may "de-identify" PHI in accordance with 45 CFR §164.514(b)(2) and use or disclose "de-identified" information in a manner consistent with and permitted by HIPAA.

**B. Prohibited Uses and Disclosures**

1. Business Associate shall not disclose PHI about an individual to a health plan for payment or health care operations purposes if the PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full and the individual requests such restriction, in accordance with 42 U.S.C. section 17935(a) and 45 CFR section 164.522(a).
2. Business Associate shall not directly or indirectly receive remuneration in exchange for PHI, except with the prior written consent of CDPH and as permitted by 42 U.S.C. section 17935(d)(2).

**C. Responsibilities of Business Associate**

Business Associate agrees:

1. **Nondisclosure.** Not to use or disclose Protected Health Information (PHI) other than as permitted or required by the Agreement or as required by law.
2. **Safeguards.** To implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI, including electronic PHI, that it creates, receives, maintains, uses or transmits on behalf of CDPH, in compliance with 45 CFR sections 164.308, 164.310 and 164.312, and to prevent use or disclosure of PHI other than as provided for by the Agreement, Business Associate shall implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of 45 CFR section 164, subpart C, in compliance with 45 CFR section 164.316. Business Associate 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 Business Associate's operations and the nature and scope of its activities, and which incorporates the requirements of section 3, Security, below. Upon written request, Business Associate will provide CDPH with the Table of Contents of its policies.
3. **Security.** To take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:

**Attachment 1**  
**HIPAA Business Associate Addendum**

- a. Complying with all of the data system security precautions listed in Attachment A, the Business Associate Data Security Requirements;
- b. Achieving and maintaining compliance with the HIPAA Security Rule (45 CFR Parts 160 and 164), as necessary in conducting operations on behalf of CDPH under the Agreement;
- c. Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III - Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and
- d. In case of a conflict between any of the security standards contained in any of these enumerated sources of security standards, the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to PHI from unauthorized disclosure. Further, Business Associate must comply with changes to these standards that occur after the effective date of the Agreement.
- e. Business Associate shall designate a Security Officer to oversee its data security program who shall be responsible for carrying out the requirements of this section and for communicating on security matters with CDPH.

**D. *Mitigation of Harmful Effects.*** To mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate or its subcontractors in violation of the requirements of this Addendum.

**E. *Business Associate's Agents and Subcontractors.***

1. To enter into written agreements with any agents, including subcontractors and vendors, to whom Business Associate provides PHI or PI received from or created or received by Business Associate on behalf of CDPH, that impose the same restrictions and conditions on such agents, subcontractors and vendors that apply to Business Associate with respect to such PHI and PI under this Addendum, and that comply with all applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations.
2. In accordance with 45 CFR section 164.504(e)(1)(ii), upon Business Associate's knowledge of a material breach or violation by its subcontractor of the agreement between Business Associate and the subcontractor, Business Associate shall:
  - a. Provide an opportunity for the subcontractor to cure the breach or end the violation and terminate the agreement if the subcontractor does not cure the breach or end the violation within the time specified by CDPH; or
  - b. Immediately terminate the agreement if the subcontractor has breached a material term of the agreement and cure is not possible.

**F. *Availability of Information to CDPH and Individuals.*** To provide access and information:

1. To provide access as CDPH may require, and in the time and manner designated by CDPH (upon reasonable notice and during Business Associate's normal business hours) to PHI in a Designated Record Set, to CDPH (or, as directed by CDPH), to an Individual, in accordance with 45 CFR section 164.524. Designated Record Set means the group of records maintained for CDPH that includes medical, dental and billing records about individuals; enrollment, payment, claims adjudication, and

**Attachment 1**  
**HIPAA Business Associate Addendum**

case or medical management systems maintained for CDPH health plans; or those records used to make decisions about individuals on behalf of CDPH. Business Associate shall use the forms and processes developed by CDPH for this purpose and shall respond to requests for access to records transmitted by CDPH within fifteen (15) calendar days of receipt of the request by producing the records or verifying that there are none.

2. If Business Associate maintains an Electronic Health Record with PHI, and an individual requests a copy of such information in an electronic format, Business Associate shall provide such information in an electronic format to enable CDPH to fulfill its obligations under the HITECH Act, including but not limited to, 42 U.S.C. section 17935(e).
3. If Business Associate receives data from CDPH that was provided to CDPH by the Social Security Administration, upon request by CDPH, Business Associate shall provide CDPH with a list of all employees, contractors and agents who have access to the Social Security data, including employees, contractors and agents of its subcontractors and agents.

**G. Amendment of PHI.** To make any amendment(s) to PHI that CDPH directs or agrees to pursuant to 45 CFR section 164.526, in the time and manner reasonably designated by CDPH.

**H. Internal Practices.** To make Business Associate's internal practices, books and records relating to the use and disclosure of PHI received from CDPH, or created or received by Business Associate on behalf of CDPH, available to the Secretary of the U.S. Department of Health and Human Services in a time and manner designated by the Secretary, for purposes of determining CDPH's compliance with the HIPAA regulations. If any information needed for this purpose is in the exclusive possession of any other entity or person and the other entity or person fails or refuses to furnish the information to Business Associate, Business Associate shall so certify to CDPH and shall set forth the efforts it made to obtain the information.

**I. Documentation of Disclosures.** To document and make available to CDPH or (at the direction of CDPH) to an Individual such disclosures of PHI, and information related to such disclosures, necessary to respond to a proper request by the subject Individual for an accounting of disclosures of PHI, in accordance with the HITECH Act and its implementing regulations, including but not limited to 45 CFR section 164.528 and 42 U.S.C. section 17935(c). If Business Associate maintains electronic health records for CDPH as of January 1, 2009, Business Associate must provide an accounting of disclosures, including those disclosures for treatment, payment or health care operations, effective with disclosures on or after January 1, 2014. If Business Associate acquires electronic health records for CDPH after January 1, 2009, Business Associate must provide an accounting of disclosures, including those disclosures for treatment, payment or health care operations, effective with disclosures on or after the date the electronic health record is acquired, or on or after January 1, 2011, whichever date is later. The electronic accounting of disclosures shall be for disclosures during the three years prior to the request for an accounting.

**J. Breaches and Security Incidents.** During the term of the Agreement, Business Associate agrees to implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and to take the following steps:

1. **Notice to CDPH.** (1) To notify CDPH promptly, without unreasonable delay, by telephone call plus email or fax upon the discovery of a breach of unsecured PHI or PI in electronic media or in any other media if the PHI or PI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, or upon the discovery of an actual security incident that involves data provided to CDPH by the Social Security Administration. (2) To notify CDPH within 48 hours by email or fax of the discovery of any actual security incident, intrusion or unauthorized access, use or

**Attachment 1**  
**HIPAA Business Associate Addendum**

disclosure of PHI or PI in violation of the Agreement and this Addendum, or potential loss of confidential data affecting the Agreement. A breach shall be treated as discovered by Business Associate as of the first day on which the breach is confirmed, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of Business Associate.

Any attempted, but unsuccessful Security Incident of which Business Associate becomes aware will be reported to Covered Entity orally or in writing upon the written reasonable request of Covered Entity. If the HIPAA Security Regulations are amended to remove the requirement to report unsuccessful attempts at unauthorized access, the requirement to report such unsuccessful attempts shall no longer apply as of the effective date of that amendment.

Notice shall be provided to the CDPH Program Contract Manager, the CDPH Privacy Officer and the CDPH Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves electronic PHI, notice shall be provided by calling the CDPH ITSD Service Desk. Notice shall be made using the "CDPH Privacy Incident Report" form, including all information known at the time. Business Associate shall use the most current version of this form, which is posted on the CDPH Privacy Office website ([www.CDPH.ca.gov](http://www.CDPH.ca.gov)).

Upon discovery of a breach or actual security incident, intrusion or unauthorized access, use or disclosure of PHI or PI, Business Associate shall take:

- a. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and
  - b. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.
2. **Investigation and Investigation Report.** To promptly, without unreasonable delay, investigate such security incident, breach, or unauthorized access, use or disclosure of PHI or PI. Within three (3) business days of the discovery, Business Associate shall submit an updated "CDPH Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Information Security Officer:
3. **Complete Report.** To provide a complete report of the investigation to the CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Information Security Officer within ten (10) working days of the confirmation of the breach or unauthorized use or disclosure. The report shall be submitted on the "CDPH Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable provisions of HIPAA, the HITECH Act, the HIPAA regulations and/or state law. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If CDPH requests information in addition to that listed on the "CDPH Privacy Incident Report" form, Business Associate shall make reasonable efforts to provide CDPH with such information. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "CDPH Privacy Incident Report" form. CDPH will review and approve the determination of whether a breach occurred and individual notifications are required, and the corrective action plan.
4. **Notification of Individuals.** If the cause of a breach of PHI or PI is attributable to Business Associate or its subcontractors, agents or vendors, Business Associate shall notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal law and shall pay

**Attachment 1**  
**HIPAA Business Associate Addendum**

any costs of such notifications, as well as any costs associated with the breach. The notifications shall comply with the requirements set forth in 42 U.S.C. section 17932 and its implementing regulations, including, but not limited to, the requirement that the notifications be made without unreasonable delay and in no event later than 60 calendar days. The CDPH Program Contract Manager, the CDPH Privacy Officer, and the CDPH Information Security Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made.

5. **Responsibility for Reporting of Breaches.** If the cause of a breach of PHI or PI is attributable to Business Associate or its agents, subcontractors or vendors, Business Associate is responsible for all required reporting of the breach as specified in 42 U.S.C. section 17932 and its implementing regulations, including notification to media outlets and to the Secretary. If a breach of unsecured PHI involves more than 500 residents of the State of California or its jurisdiction, Business Associate shall notify the Secretary of the breach promptly upon discovery of the breach. If Business Associate has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to CDPH in addition to Business Associate, Business Associate shall notify CDPH, and CDPH and Business Associate may take appropriate action to prevent duplicate reporting. The breach reporting requirements of this paragraph are in addition to the reporting requirements set forth in subsection 1, above.
6. **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 giving written notice to the Contractor. Said changes shall not require an amendment to this Addendum or the Agreement to which it is incorporated.

CDPH Program Contract Manager	CDPH Privacy Officer	CDPH Information Security Officer
See the Scope of Work exhibit for Program Contract Manager information	Privacy Officer Privacy Office, c/o Office of Legal Services California Department of Public Health 1415 L Street, 5 <sup>th</sup> Floor Sacramento, CA 95814  Email: <a href="mailto:privacy@cdph.ca.gov">privacy@cdph.ca.gov</a> Telephone: (877) 421-9634	Chief Information Security Officer Information Security Office California Department of Public Health P.O. Box 997413, MS 6302 Sacramento, CA 95899-7413  Email: <a href="mailto:cdphiso@cdph.ca.gov">cdphiso@cdph.ca.gov</a> Telephone: IT Service Desk (916) 440-7000 or (800) 579-0874

**Attachment 1**  
**HIPAA Business Associate Addendum**

**K. Termination of Agreement.** In accordance with Section 13404(b) of the HITECH Act and to the extent required by the HIPAA regulations, if Business Associate knows of a material breach or violation by CDPH of this Addendum, it shall take the following steps:

1. Provide an opportunity for CDPH to cure the breach or end the violation and terminate the Agreement if CDPH does not cure the breach or end the violation within the reasonable time specified by Business Associate; or
2. Immediately terminate the Agreement if CDPH has breached a material term of the Addendum and cure is not possible.

**L. Due Diligence.** Business Associate shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this Addendum and is in compliance with applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations, and that its agents, subcontractors and vendors are in compliance with their obligations as required by this Addendum.

**M. Sanctions and/or Penalties.** Business Associate understands that a failure to comply with the provisions of HIPAA, the HITECH Act and the HIPAA regulations that are applicable to Business Associate may result in the imposition of sanctions and/or penalties on Business Associate under HIPAA, the HITECH Act and the HIPAA regulations.

**IV. Obligations of CDPH**

CDPH agrees to:

- A. Notice of Privacy Practices.** Provide Business Associate with the Notice of Privacy Practices that CDPH produces in accordance with 45 CFR section 164.520, as well as any changes to such notice.
- B. Permission by Individuals for Use and Disclosure of PHI.** Provide the Business Associate with any changes in, or revocation of, permission by an Individual to use or disclose PHI, if such changes affect the Business Associate's permitted or required uses and disclosures.
- C. Notification of Restrictions.** Notify the Business Associate of any restriction to the use or disclosure of PHI that CDPH has agreed to in accordance with 45 CFR section 164.522, to the extent that such restriction may affect the Business Associate's use or disclosure of PHI.
- D. Requests Conflicting with HIPAA Rules.** Not request the Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA regulations if done by CDPH.

**V. Audits, Inspection and Enforcement**

- A.** From time to time, Business Associate agrees to make its security policies Table of Contents or redacted copies of its policies and procedures available to CDPH upon written request to monitor Business Associate's compliance with the Agreement and this Addendum. Business Associate shall promptly remedy any violation of any provision of this Addendum and shall certify the same to the CDPH Privacy Officer in writing. The fact that CDPH inspects, or fails to inspect, or has the right to inspect, Business Associate's policies and procedures does not relieve Business Associate of its responsibility to comply with this Addendum, nor does CDPH's:

**Attachment 1**  
**HIPAA Business Associate Addendum**

1. Failure to detect or
2. Detection, but failure to notify Business Associate or require Business Associate's remediation of any unsatisfactory practices constitute acceptance of such practice or a waiver of CDPH' enforcement rights under the Agreement and this Addendum.

**B.** If Business Associate is the subject of an audit, compliance review, or complaint investigation by the Secretary or the Office of Civil Rights, U.S. Department of Health and Human Services, that is related to the performance of its obligations pursuant to this HIPAA Business Associate Addendum, Business Associate shall notify CDPH and provide CDPH with a copy of any PHI or PI that Business Associate provides to the Secretary or the Office of Civil Rights concurrently with providing such PHI or PI to the Secretary. Business Associate is responsible for any civil penalties assessed due to an audit or investigation of Business Associate, in accordance with 42 U.S.C. section 17934(c).

## **VI. Termination**

**A. Term.** The Term of this Addendum shall commence as of the effective date of this Addendum and shall extend beyond the termination of the Agreement and shall terminate when all the PHI provided by CDPH to Business Associate, or created or received by Business Associate on behalf of CDPH, is destroyed or returned to CDPH, in accordance with 45 CFR 164.504(e)(2)(ii)(I).

**B. Termination for Cause.** In accordance with 45 CFR section 164.504(e)(1)(ii), upon CDPH' knowledge of a material breach or violation of this Addendum by Business Associate, CDPH shall:

1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate the Agreement if Business Associate does not cure the breach or end the violation within the reasonable time specified by CDPH; or
2. Immediately terminate the Agreement if Business Associate has breached a material term of this Addendum and cure is not possible.

**C. Judicial or Administrative Proceedings.** Business Associate will notify CDPH if it is named as a defendant in a criminal proceeding for a violation of HIPAA. CDPH may terminate the Agreement if Business Associate is found guilty of a criminal violation of HIPAA. CDPH may terminate the Agreement if a finding or stipulation that the Business Associate has violated any standard or requirement of HIPAA, or other security or privacy laws is made in any administrative or civil proceeding in which the Business Associate is a party or has been joined.

**D. Effect of Termination.** Upon termination or expiration of the Agreement for any reason, Business Associate shall return or destroy all PHI received from CDPH (or created or received by Business Associate on behalf of CDPH) that Business Associate still maintains in any form, and shall retain no copies of such PHI. If return or destruction is not feasible, Business Associate shall notify CDPH of the conditions that make the return or destruction infeasible, and CDPH and Business Associate shall determine the terms and conditions under which Business Associate may retain the PHI. Business Associate shall continue to extend the protections of this Addendum to such PHI, and shall limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate.

## **VII. Miscellaneous Provisions**

**A. Disclaimer.** CDPH makes no warranty or representation that compliance by Business Associate with this Addendum, HIPAA or the HIPAA regulations will be adequate or satisfactory for Business Associate's own purposes or that any information in Business Associate's possession or control, or transmitted or

**Attachment 1**  
**HIPAA Business Associate Addendum**

received by Business Associate, is or will be secure from unauthorized use or disclosure. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI.

- B. Amendment.** The parties acknowledge that federal and state laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Addendum may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, the HIPAA regulations and other applicable laws relating to the security or privacy of PHI. Upon CDPH' request, Business Associate agrees to promptly enter into negotiations with CDPH concerning an amendment to this Addendum embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, the HIPAA regulations or other applicable laws. CDPH may terminate the Agreement upon thirty (30) days written notice in the event:
1. Business Associate does not promptly enter into negotiations to amend this Addendum when requested by CDPH pursuant to this Section; or
  2. Business Associate does not enter into an amendment providing assurances regarding the safeguarding of PHI that the parties mutually deem sufficient to satisfy the standards and requirements of HIPAA and the HIPAA regulations.
- C. Assistance in Litigation or Administrative Proceedings.** Business Associate shall make itself and any subcontractors, employees or agents assisting Business Associate in the performance of its obligations under the Agreement, available to CDPH at no cost to CDPH to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CDPH, its directors, officers or employees based upon claimed violation of HIPAA, the HIPAA regulations or other laws relating to security and privacy, which involves inactions or actions by the Business Associate, except where Business Associate or its subcontractor, employee or agent is a named adverse party.
- D. No Third-Party Beneficiaries.** Nothing express or implied in the terms and conditions of this Addendum is intended to confer, nor shall anything herein confer, upon any person other than CDPH or Business Associate and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.
- E. Interpretation.** The terms and conditions in this Addendum shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, the HIPAA regulations and applicable state laws. The parties agree that any ambiguity in the terms and conditions of this Addendum shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act and the HIPAA regulations.
- F. Regulatory References.** A reference in the terms and conditions of this Addendum to a section in the HIPAA regulations means the section as in effect or as amended.
- G. Survival.** The respective rights and obligations of Business Associate under Section VI.D of this Addendum shall survive the termination or expiration of the Agreement.
- H. No Waiver of Obligations.** No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.



**Attachment**  
**HIPAA Business Associate Addendum**

**Attachment A**  
**Business Associate Data Security Requirements**

**I. Personnel Controls**

- A. *Employee Training.*** All workforce members who assist in the performance of functions or activities on behalf of CDPH, or access or disclose CDPH PHI or PI must complete information privacy and security training, at least annually, at Business Associate's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following contract termination.
- B. *Employee Discipline.*** Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.
- C. *Confidentiality Statement.*** All persons that will be working with CDPH PHI or PI must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to CDPH PHI or PI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for CDPH inspection for a period of six (6) years following contract termination. The confidentiality statement must be provided to Business Associate by CDPH upon start of the Agreement and annually thereafter.
- D. *Workforce Member Assessment.*** Before a member of the Contractor's workforce may access CDPH PCI, Contractor must ensure that all workforce members that will have access to CDPH PCI have been assessed to assure that there is no indication that the workforce member may present a risk to the security or integrity of CDPH PCI. Contractor shall retain each workforce member's assessment documentation, whether in physical or electronic format, for a period of three (3) years following contract termination.

**II. Technical Security Controls**

- A. *Workstation/Laptop encryption.*** All workstations and laptops that process and/or store CDPH PHI or PI must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the CDPH Information Security Office.
- B. *Server Security.*** Servers containing unencrypted CDPH PHI or PI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.
- C. *Minimum Necessary.*** Only the minimum necessary amount of CDPH PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.
- D. *Removable media devices.*** All electronic files that contain CDPH PHI or PI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, Blackberry, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.

**Attachment \_**  
**HIPAA Business Associate Addendum |**

- E. **Antivirus software.** All workstations, laptops and other systems that process and/or store CDPH PHI or PI must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.
- F. **Patch Management.** All workstations, laptops and other systems that process and/or store CDPH PHI or PI must have critical 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 except in situations when assessed risk is considered to be too high.
- G. **User IDs and Password Controls.** All users must be issued a unique user name for accessing CDPH PHI or PI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within 24 hours. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every 90 days, preferably every 60 days. Passwords must be changed if revealed or compromised. Passwords 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)
- H. **Data Destruction.** When no longer needed, all CDPH PHI or PI must be wiped using the Gutmann or US Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission of the CDPH Information Security Office.
- I. **System Timeout.** The system providing access to CDPH PHI or PI must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.
- J. **Warning Banners.** All systems providing access to CDPH PHI or PI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.
- K. **System Logging.** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for CDPH PHI or PI, or which alters CDPH PHI or PI. 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. If CDPH PHI or PI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.
- L. **Access Controls.** The system providing access to CDPH PHI or PI must use role based access controls for all user authentications, enforcing the principle of least privilege.

**Attachment \_**  
**HIPAA Business Associate Addendum**

- M. *Transmission encryption.*** All data transmissions of CDPH PHI or PI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing PHI can be encrypted. This requirement pertains to any type of PHI or PI in motion such as website access, file transfer, and E-Mail.
- N. *Intrusion Detection.*** All systems involved in accessing, holding, transporting, and protecting CDPH PHI or PI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

### **III. Audit Controls**

- A. *System Security Review.*** All systems processing and/or storing CDPH PHI or PI 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 should include vulnerability scanning tools.
- B. *Log Reviews.*** All systems processing and/or storing CDPH PHI or PI must have a routine procedure in place to review system logs for unauthorized access.
- C. *Change Control.*** All systems processing and/or storing CDPH PHI or PI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

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

- A. *Emergency Mode Operation Plan.*** Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic CDPH PHI or PI 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 the Agreement for more than 24 hours.
- B. *Data Backup Plan.*** Contractor must have established documented procedures to backup CDPH PHI to maintain retrievable exact copies of CDPH PHI or PI. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore CDPH PHI or PI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of CDPH data.

### **V. Paper Document Controls**

- A. *Supervision of Data.*** CDPH PHI or PI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. CDPH PHI or PI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.
- B. *Escorting Visitors.*** Visitors to areas where CDPH PHI or PI is contained shall be escorted and CDPH PHI or PI shall be kept out of sight while visitors are in the area.
- C. *Confidential Destruction.*** CDPH PHI or PI must be disposed of through confidential means, such as cross cut shredding and pulverizing.

**Attachment \_**  
**HIPAA Business Associate Addendum |**

- D. *Removal of Data.*** CDPH PHI or PI must not be removed from the premises of the Contractor except with express written permission of CDPH.
- E. *Faxing.*** Faxes containing CDPH PHI or PI 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 the fax.
- F. *Mailing.*** Mailings of CDPH PHI or PI shall be sealed and secured from damage or inappropriate viewing of PHI or PI to the extent possible. Mailings which include 500 or more individually identifiable records of CDPH PHI or PI 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.