SCO ID: 7760-24209710-1

STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES
STANDARD AGREEMENT
STD 213 (Rev. 04/2020)

AGREEMENT NUMBER	PURCHASING AUTHORITY NUMBER (If Applicable)
24-209710-1	

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

CONTRACTING AGENCY NAME
Department of General Services- Office of Administrative Hearings

CONTRACTOR NAME
Cal Interpreting & Translations

2. The term of this Agreement is:

START DATE
October 18, 2024 or upon DGS/OBAS Approval whichever is later

THROUGH END DATE
April 17, 2025

3. The maximum amount of this Agreement is:
$96,940.00 Ninety-Six Thousand Nine Hundred Forty Dollars and Zero Cents

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

Exhibits	Title	Pages
Exhibit A	Scope of Work	9
Exhibit A, Attachment 1	Office of Administrative Hearings Locations	1
Exhibit A, Attachment 2	Office of Administrative Hearings Regions	1
Exhibit B	Budget Detail and Payment Provisions	2
Exhibit B, Attachment 1	Cost Sheet	6
Exhibit C *	General Terms and Conditions	GTC 04/2017
Exhibit D	Special Terms and Conditions	5
Exhibit E	Additional Provisions	2
Exhibit F	Data Processing and Data Protection	4
Exhibit G	Additional Provision for Specific OAH Case Types	2
Exhibit G, Attachment 1-4	As identified on the specific attachment	51

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.)
Cal Interpreting & Translations

CONTRACTOR BUSINESS ADDRESS	CITY	STATE	ZIP
5990 Sepulveda Blvd., Suite 250	Van Nuys	CA	91411

PRINTED NAME OF PERSON SIGNING	TITLE
Igal saidian	President

CONTRACTOR AUTHORIZED SIGNATURE	DATE SIGNED
Igal saidian Igal Saidian (Oct 21, 2024 09:29 PDT)	10/21/2024

SCO ID: 7760-24209710-1

STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES
STANDARD AGREEMENT
STD 213 (Rev. 04/2020)

AGREEMENT NUMBER	PURCHASING AUTHORITY NUMBER (If Applicable)
24-209710-1	

STATE OF CALIFORNIA

CONTRACTING AGENCY NAME
Department of General Services

CONTRACTING AGENCY ADDRESS	CITY	STATE	ZIP
707 3rd Street	West Sacramento	CA	95605

PRINTED NAME OF PERSON SIGNING	TITLE
Tim Dean	Staff Services Manager I

CONTRACTING AGENCY AUTHORIZED SIGNATURE	DATE SIGNED
Tim Dean Tim Dean (Oct 21, 2024 13:30 PDT)	10/21/2024

CALIFORNIA DEPARTMENT OF GENERAL SERVICES APPROVAL	EXEMPTION (If Applicable)
10/22/2024	Exempt from DGS/OLS' Approval per DGS Exemption Letter

DEPARTMENT OF GENERAL SERVICES
AD-OBAS
APPROVED

EXHIBIT A

SCOPE OF WORK

The Administrative Law Judges (ALJs) from the Office of Administrative Hearings conduct administrative hearings in accordance with Government Code sections 11500 et seq., other applicable statutes, and pursuant to contracts and interagency agreements with other state and local entities. The State of California, Department of General Services, Office of Administrative Hearings (OAH or State) requires Certified, Registered, or Qualified, as described herein, court interpreter and document translation services for various court proceedings and other events.

1. Project Summary

A. Upon request, Contractor shall provide language professionals, equipment, materials and tools required for OAH proceedings (i.e., committees, conferences, mediations and hearings) for the following:

   1) Interpreting Services:
      a. Onsite/In-person Interpreters
      b. Telephonic/Video/Remote interpreting (VRI)
   2) Document Translation

B. The Contractor will provide these services covering proceedings in the Northern Region.

C. This contract is subject to Data Processing and Protection as outlined in Exhibit F and has additional provisions for specific OAH case types as identified in Exhibit G and its attachments.

D. On-site/In-person interpreter services shall take place at an OAH office location and at other locations in the State of California as set by OAH. OAH office locations are identified in Exhibit A, Attachment 1. Other locations may include regional centers (non-profit corporations under contract with the Department of Developmental Services), school district offices, and other state or local agency office locations.

E. The State will have the sole option to extend the Agreement term for one additional six-month term at the contracted rates.

2. Contract Administrators

A. The Contract Administrators during the term of this Agreement will be:

OAH Contract Administrator	Contractor's Contract Administrator
Phoenix Lawson 2349 Gateway Oaks Drive Suite 200 Sacramento, CA 95833 Phone: **REDACTED** Email: **REDACTED**	Ida Zaghi, Director of Contracting 5990 Sepulveda Blvd. Ste. 250 Van Nuys, CA 91411-2548 Phone: **REDACTED** Email: **REDACTED**

B. The State reserves the right to identify an OAH Designated Representative in the absence of the OAH Contract Administrator.

C. Any changes in Contractor's Contract Administrator must be immediately reported in writing to the OAH Contract Administrator or OAH Designated Representative.

3. Minimum Qualifications

A. For purposes of this Agreement the following definitions will be used:

1) "Certified" shall mean that the person providing the language services is certified by the State of California's Judicial Council and/or included on the California Department of Human Resources' interpreter listing.

2) "Registered" shall mean that the person providing the language services is designated as a registered interpreter by the State of California's Judicial Council.

3) "Qualified" shall mean that Contractor reasonably and in good faith believes that the person providing the language services has sufficient interpreting skills and linguistic abilities in the language for which they have been designated by Contractor for the person providing language services to be provisionally qualified and used for an Administrative Hearing or other proceeding pursuant to Government Code section 11435.55, even though the person providing language services is not a Certified or Registered interpreter. In the event that Contractor schedules Qualified language services, the person providing language services shall be deemed provisionally qualified pursuant to Government Code section 11435.55, subdivision (a).

4) Interpreters providing services must be regularly employed by the Contractor or under contract.

4. Definitions

A. "Simultaneous interpretation" shall mean when an interpreter translates, in real-time, the message in the source language to the target language. It is the State's understanding that simultaneous interpretation events scheduled for longer than one hour will require two interpreters.

B. "Consecutive interpretation" shall mean interpreting that is done by listening to what the speaker is saying and then conveying the message into another language after the speaker has paused talking. It is the State's understanding that consecutive interpretation events require one interpreter regardless of the length of the event.

5. Privacy and Information Security

A. Contractor agrees to maintain a working personal or business e-mail account for purposes of communications relating to this Agreement only.

B. Contractor, and Contractor's agents, employees and/or subcontractors as appropriate and as determined by DGS, will be provided access to one or more DGS accounts for purposes of transmittal of case information. Contractor shall use the account provided by DGS for exchanges of all case-related information, including case files and invoicing, between Contractor and OAH.

C. DGS' Information Security Office mandates all persons with access to DGS accounts complete training on privacy and information security annually. If training is not completed, DGS may revoke Contractor's account access and OAH may suspend all work under this Agreement.

D. Contractor is responsible for abiding by all DGS privacy and information security requirements, including maintaining a secure password, timely completing any training(s) assigned by OAH or DGS regarding privacy or information security, and supplying confirmation of such training(s) upon request to the OAH Contract Administrator or designee. No payment will be provided for privacy or information security training.

E. Contractor agrees DGS accounts are only for the exchange of information between Contractor and OAH and not to be used in any way for other commercial, professional or personal purposes.

6. Service Details

A. Contractor will provide interpreters for services between the hours of 8:00 a.m. to 6:00 p.m. (PT), Monday through Friday with the exception of holidays unless otherwise stated in the request for service. The length of the court proceedings or other assignment will vary from thirty (30) minutes to several weeks.

B. Current observed State holidays are: New Year's Day, Martin Luther King, Jr. Day, President's Day, Cesar Chavez Day, Memorial Day, Independence Day, Labor Day, Veteran's Day, Thanksgiving Day, Day after Thanksgiving and Christmas Day.

C. Contractor shall provide interpreters via VRI as requested by OAH. For the VRI services, interpreting will be done remotely in the method required by OAH (i.e., Zoom, Teams, live-stream webinar, videoconference, chat, telephone, etc.).

D. If, after Contractor's reasonable and good faith attempt to obtain Certified or Registered language services, Contractor is unable to provide Certified or Registered language services for a particular assignment because of the unavailability of a Certified or Registered language interpreter, Contractor may assign a Qualified interpreter.

   1) In the event of assignment of a Qualified interpreter, Contractor shall notify the OAH Requestor of the unavailability of a Certified or Registered interpreter by email, no later than 12:00 p.m. (noon) three business days before the scheduled assignment, or as soon as practicable if the OAH Requestor made the request in three or fewer business days before the scheduled assignment or deadline for language services.

E. Contractor will provide all labor, materials, tools, and equipment, and shall pay all expenses including, but not limited to, travel mileage, parking, taxes, insurance, bonds, license and permit fees, and any other costs incidental to providing the services.

F. Contractor shall provide written translations of source texts provided from English into another language within the meaning and intent of the original text. Services shall include translation of documentation by Certified interpreters, Registered interpreters, or Qualified interpreters subject to the provisions of Paragraph 6.D. above.

G. The most commonly requested languages for interpreter and document translation services are listed below, as well as on Exhibit B, Attachment 1, Cost Sheet. The Cost Sheet shall have the rate charges for simultaneous interpretation and consecutive interpretation. Languages not specifically identified below and on the Cost Sheets may be charged at a rate selected solely by the Contractor but shall not exceed the highest rate on Exhibit B, Attachment 1, Cost Sheet, for the same service and same timeframe.

- Arabic
- Armenian
- Chinese (including Mandarin and Cantonese)
- Farsi (Persian)
- Filipino (Tagalog)
- Japanese
- Khmer
- Korean
- Portuguese
- Punjabi (India)
- Russian
- Spanish
- Vietnamese

H. The expertise required is for interpretation of legal/court administrative hearings or proceedings and translation of legal documents such as:

1) Notice of Continuance
2) Notice of Mediation
3) Notice of Hearing and Mediation
4) Dismissal Order
5) Decision or Proposed Decision
6) Due Process Complaint
7) Fair Hearing or Appeal Request
8) Procedural Safeguards

Note: Additional documents may be required as the need arises.

I. An OAH Proceeding can include a determination of competence of a wide range of professions (e.g., physicians and other medical professionals, certified public accountants, engineers, contractors) and determination of eligibility for services or appropriate services for children, adults, and students with disabilities. Contractor is expected to provide language services that include awareness of technical and disability terminology, in addition to abiding by all requirements set forth in this Agreement, including all exhibits.

J. OAH does not guarantee the amount of work or services that may be requested from Contractor. The estimated number of hours provided in Exhibit B, Attachment 1 Cost Sheet is only an estimate. The State reserves the right to increase or decrease the amount based on actual need of services.

K. The State reserves the right to obtain services outside this contract if needed.

7. Building Security

A. The State shall have and exercise full and complete control over granting, denying, withholding or terminating building clearances for Contractor's personnel.

B. Depending on the location of the hearing, Contractor's staff may be required to check in with building security at the buildings main entrance or reception, where they may be required to provide a valid State of California issued identification. In the event the building security or reception issues Contractor's personnel a

temporary pass, the temporary pass shall be worn while performing services in the building and on building's grounds and returned at the end of each day.

8. **Scheduling Details**

A. Whenever possible, OAH shall provide at least three (3) calendar days' notice to Contractor, by either telephone or email request, for interpreter services. The request shall include:
   1) OAH Requestor's Name, email address and phone number,
   2) type of service requested
   3) language requested,
   4) if simultaneous or consecutive interpretation is required,
   5) nature of the proceeding (e.g. mediation, prehearing conference, hearing, etc.),
   6) date(s), time, and, if in-person, the location of hearing,
   7) name of assigned ALJ (if assigned),
   8) OAH Case Number, and
   9) OAH Case Name.

B. OAH will request document translation services via email with an electronic version of the document. The request shall include:
   1) OAH Requestor's Name, email address and phone number,
   2) language requested,
   3) OAH Case Name,
   4) OAH Case Number,
   5) original word count of document, if known,
   6) requested turn-around time, and
   7) name of document.

C. Interpreter Services Requests

   a. Within 24 hours of receipt of a request for services, Contractor shall reply by email to the OAH Requestor confirming receipt of the request.

   b. Contractor shall email the OAH Requestor when Contractor has assigned an interpreter for the requested service. The email shall include the name, email address and telephone number of the assigned interpreter, and clearly state whether the interpreter is Certified, Registered, or Qualified (see Paragraph 3.A.). Contractor shall confirm assignment of the interpreter no later than four (4) full business days before the date of the event for which the assignment is needed, unless OAH has requested the interpreter less than four business days before the event.

D. Document Translation Requests

a. Within 24 hours of receipt of a request for services, Contractor shall reply by email to the OAH Requestor confirming receipt of the request.

b. Contractor shall email the OAH Requestor when Contractor has assigned an interpreter for the requested service. The email shall clearly state whether the assigned interpreter is Certified, Registered, or Qualified (see Paragraph 3.A.).

c. The turnaround time for document translations shall not be longer than the time stated in the request (i.e., 24 or 48 hours).

i. In the event Contractor requires additional time to complete the request, Contractor shall email the OAH Requestor to advise an extension is needed, the reason for the extension, and the date Contractor anticipates the request will be completed.
ii. If Contractor's anticipated completion date is unacceptable to OAH, OAH shall immediately notify Contractor and Contractor shall immediately cease any further work on the request. In such event, OAH shall be responsible for any work performed by Contractor until OAH's notification to Contractor.

d. Contractor shall complete the requested document translation and return the translated document via email to the OAH Requestor in both Word and PDF format. Email communication is identified in Section 5.

E. Scheduled events are subject to change. The OAH Contract Administrator or OAH Designated Representative and Contractor shall mutually agree in writing to modify scheduled events, as needed, to reasonably accommodate the completion of the proceeding.

9. **Performance Details**

A. Accuracy

1) Contractor is responsible for ensuring the quality and accuracy of all interpreters and document translation services.

2) Contractor agrees to:
i. Proofread all translations for typographical errors and accuracy;
ii. Review document translations for content to ensure that the intent of the original document is maintained; and
iii. Review document translations for errors in choice of words and phrases, syntax and grammar.

3) Corrections and changes to translated documents requested by OAH shall be completed in a timely fashion at no cost to OAH.

B. Late Arrivals

1) Contractor is responsible for ensuring that interpreters arrive and begin participating at the scheduled time for OAH court proceedings.

2) OAH, in its discretion, may report a late arrival (the incident) to the Judicial Council of California, California Court Interpreters Program, the California Department of Human Resources, and/or DGS. For purposes of this section, a late arrival is defined as arriving or starting participation in an OAH proceeding fifteen (15) minutes or more after the scheduled start time of an OAH proceeding.

C. Contractor shall ensure the interpreters adhere to the following:

1) Will maintain an impartial, professional relationship with all court officers, attorneys, parties, and witnesses and accurately interpret the proceedings.

2) Will not disclose privileged communications between counsel and client to any person.

3) Will not give legal advice to parties and witnesses, nor recommend specific attorneys or law firms, or embellish communications in any way.

4) Will accurately interpret the participant's statements and relay the message in its entirety with the meaning preserved throughout the conversation. Information will not be edited or deleted which may erroneously change the meaning of the participant's statements.

5) Will wear business attire to OAH proceedings. Refrain from wearing items such as jeans, and shorts, and for in person events, tennis shoes.

D. Liquidated Damages

1. In the event that Contractor fails to deliver in accordance with the Agreement requirements, the parties agree that the delay will interfere with the proper implementation of the State's programs, to the loss and damage of the State. From the nature of the proceedings before OAH, it would be impracticable and extremely difficult to fix the actual damages sustained in the event of any such delay. The State and Contractor, therefore, agree that in the event of any such delay the amount of damage which will be sustained from a delay will be $300 per incident, and the State and Contractor agree that in the event of any such delay, Contractor shall pay such amounts as liquidated damages and not as a penalty. Amounts due to the State as liquidated damages may

be deducted by the State from any money payable to Contractor. The State shall notify Contractor in writing of any claim for liquidated damages pursuant to this paragraph on or before the date the State deducts such sums from money payable to Contractor.

10. Cancellations/Overages

A. If a service is requested and accepted by a Contractor, then cancelled by OAH the following cancellation fees shall apply:

   1) Cancellations more than 48 hours prior to the scheduled time will incur no cancellation fee;
   2) Cancellations 48 hours or less, but more than, or equal to, 24 hours prior to the time scheduled will incur a charge equal to half of the service charge scheduled for that day; and
   3) Cancellations less than 24 hours prior to the scheduled time will be charged for the time scheduled for that day.

B. In the event an interpreter service appointment lasts more than 15 minutes over the originally scheduled four (4) or eight (8) hour time frame, the supplementary service will be charged as an additional four (4) hour service at the same language rate as the original request.

C. This Agreement may be canceled in whole or in part without cause by OAH upon thirty (30) days' written notice to Contractor. In the event of early termination, Contractor shall be paid for services rendered up to the cancellation date at the rates identified in Exhibit B, Attachment 1.

EXHIBIT A, ATTACHMENT 1

OFFICE OF ADMINISTRATIVE HEARINGS LOCATIONS

General Jurisdiction Division

SACRAMENTO 2349 Gateway Oaks Drive, Suite 200 Sacramento, CA 95833 Phone: (916) 263-0550	LOS ANGELES 320 West Fourth Street, Room 630 Los Angeles, CA 90013 Phone: (213) 576-7200
OAKLAND 1515 Clay Street, Suite 206 Oakland, CA 94612 Phone: (510) 622-2722	SAN DIEGO 402 West Broadway, Suite 600 San Diego, CA 92101 Phone: (619) 525-4475

Special Education Division

SACRAMENTO 2349 Gateway Oaks Drive, Suite 200 Sacramento, CA 95833 Phone: (916) 263-0880	LOS ANGELES 355 South Grand Avenue, Suite 2200 Los Angeles, CA 90071 Phone: (916) 263-0880
OAKLAND 1515 Clay Street, Suite 206 Oakland, CA 94612 Phone: (916) 263-0880	SAN DIEGO 402 West Broadway, Suite 600 San Diego, CA 92101 Phone: (916) 263-0880

THE REST OF THIS PAGE IS BLANK

EXHIBIT A, ATTACHMENT 2

OFFICE OF ADMINISTRATIVE HEARINGS REGIONS

Northern Region – by County

Alameda	Alpine	Amador	Butte
Calaveras	Colusa	Contra Costa	Del Norte
El Dorado	Fresno	Glenn	Humboldt
Kings	Lake	Lassen	Madera
Marin	Mariposa	Mendocino	Merced
Modoc	Mono	Monterey	Napa
Nevada	Placer	Plumas	Sacramento
San Benito	San Francisco	San Joaquin	San Mateo
Santa Clara	Santa Cruz	Shasta	Sierra
Siskiyou	Solano	Sonoma	Stanislaus
Sutter	Tehama	Trinity	Tulare
Tuolumne	Yolo	Yuba	

Southern Region – by County

Kern	Imperial	Inyo	Los Angeles
Orange	Riverside	San Bernardino	San Diego
San Luis Obispo	Santa Barbara	Ventura	

EXHIBIT B

BUDGET DETAIL AND PAYMENT PROVISIONS

1. INVOICING AND PAYMENT

A. For services satisfactorily rendered, and upon receipt and approval of the invoices, the State agrees to compensate the Contractor in accordance with the rates specified in Exhibit B, Attachment 1, Cost Sheet.

B. Payment shall be made in arrears. Contractor shall submit invoices no later than the 5th of the month following the month the services were provided. Contractor shall submit invoices in Excel format no more than monthly to **REDACTED**. Invoices for interpreting and document translation services may be submitted separately.

C. Invoices shall be on company letterhead and shall include:

1) Contractor's Name
2) Contractor's Address
3) Contractor's Phone Number
4) Agreement Number
5) Date of Invoice
6) Date the order was received
7) Name of OAH employee who made request
8) OAH Case Name
9) OAH Case Number
10) Date(s) of scheduled service
11) Date and time cancellation notice received, if applicable
12) Language provided
13) Name of interpreter/translator who provided service
14) Type of Service (In-Person Interpreting, Telephonic Interpreting, Video Remote Interpreting, Document Translation)
15) Type of Service, Simultaneous or consecutive translation.
16) Applicable rate
17) Total dollar amount of invoice
18) If Contractor is a California Certified Small Business (SB), invoice will be marked clearly stating that they are a California Certified SB and will include their Certification Reference Number

D. Should an invoice be disputed, Contractor will correct any/all disputed items on the invoice and resubmit the invoice as indicated above. Failure to provide and resubmit a corrected invoice will result in a delay of payment. Under no circumstances will a credit memo be accepted in lieu of a corrected invoice.

2. BUDGET CONTINGENCY CLAUSE

A. This Agreement is valid and enforceable only if sufficient funds are made available by the Budget Act of the appropriate fiscal year for the purpose of this program.

B. It is mutually agreed that if the Budget Act of the current year and/or any subsequent years covered under this Agreement does not appropriate sufficient funds for the program, this Agreement shall be of no further force and effect. In this event, the State shall have no liability to pay any funds whatsoever to Contractor or to furnish any other considerations under this Agreement and Contractor shall not be obligated to perform any provisions of this Agreement.

C. If funding for any fiscal year is reduced or deleted by the Budget Act for purposes of this program, the State shall have the option to either cancel this Agreement with no liability occurring to the State or offer an Agreement Amendment to Contractor to reflect the reduced amount.

D. This Agreement is subject to any additional restrictions, limitations or conditions enacted by the Legislature that may affect the provisions, terms or funding of this Agreement in any manner.

3. PROMPT PAYMENT CLAUSE

A. Payment will be made in accordance with, and within the time specified in, Government Code, chapter 4.5, commencing with section 927.

4. CONTRACTOR OVERPAYMENTS

A. If the State determines that an overpayment has been made to Contractor, the State will seek recovery immediately upon discovery of the overpayment by: (a) calling Contractor's accounting office to request a refund of the overpayment amount, or (b) offsetting subsequent Contractor payments by the amount of the overpayment if Contractor repayment or credit is not received within thirty (30) days from the date of notice.

B. If Contractor discovers they have received an overpayment, Contractor must notify the State and refund the overpayment immediately.

THE REST OF THIS PAGE IS BLANK

EXHIBIT B, ATTACHMENT 1

COST SHEET- Northern Region

1. CERTIFIED/QUALIFIED/REGISTERED IN-PERSON SIMULTANEOUS INTERPRETER RATES

	A	B	C	D	E	F
Language	**Full-Day Rate (8 hours) [1]**	**Estimated Quantity**	**Half-Day Rate (4 hours) [1]**	**Estimated Quantity**	**Number of Interpreters**	**Calculated Amount (AxB) + (CxD) x E**
Arabic	$250.00	1	$200.00	1	2	$900.00
Armenian	$250.00	1	$200.00	1	2	$900.00
Chinese (including Mandarin and Cantonese)	$250.00	2	$200.00	2	2	$1,800.00
Farsi (Persian)	$250.00	1	$200.00	1	2	$900.00
Filipino (Tagalog)	$250.00	1	$200.00	1	2	$900.00
Japanese	$250.00	1	$200.00	1	2	$900.00
Khmer	$250.00	1	$200.00	1	2	$900.00
Korean	$250.00	1	$200.00	1	2	$900.00
Portuguese	$190.00	1	$160.00	1	2	$700.00
Punjabi (India)	$250.00	1	$200.00	1	2	$900.00
Russian	$250.00	1	$200.00	1	2	$900.00
Spanish	$250.00	10	$200.00	5	2	$7,000.00
Vietnamese	$250.00	1	$200.00	1	2	$900.00
Certified/Qualified/Registered In-Person Simultaneous Interpreter Total (Sum of Column F)						$18,500.00

[1]Rates are for one interpreter; however, due to the length of events, it is the State's understanding that two interpreters will be required for all simultaneous assignments over one hour.

2. CERTIFIED/QUALIFIED/REGISTERED IN-PERSON CONSECUTIVE INTERPRETER RATES

	A	B	C	D	E
Language	**Full-Day Rate (8 hours)**	**Estimated Quantity**	**Half-Day Rate (4 hours)**	**Estimated Quantity**	**Calculated Amount (AxB) + (CxD)**
Arabic	$250.00	1	$200.00	1	$450.00
Armenian	$250.00	1	$200.00	1	$450.00
Chinese (including Mandarin and Cantonese)	$250.00	2	$200.00	2	$900.00
Farsi (Persian)	$250.00	1	$200.00	1	$450.00
Filipino (Tagalog)	$250.00	1	$200.00	1	$450.00
Japanese	$250.00	1	$200.00	1	$450.00
Khmer	$250.00	1	$200.00	1	$450.00
Korean	$250.00	1	$200.00	1	$450.00
Portuguese	$190.00	1	$160.00	1	$350.00
Punjabi (India)	$250.00	1	$200.00	1	$450.00
Russian	$250.00	1	$200.00	1	$450.00
Spanish	$250.00	20	$200.00	10	$7,000.00
Vietnamese	$250.00	1	$200.00	1	$450.00
Certified/Qualified/Registered In-Person Consecutive Interpreter Total (Sum of Column E)					$12,750.00

3. CERTIFIED/QUALIFIED/REGISTERED VIRTUAL SIMULTANEOUS INTERPRETER RATES

	A	B	C	D	E	F
Language	**Full-Day Rate (8 hours) [1]**	**Estimated Quantity**	**Half-Day Rate (4 hours) [1]**	**Estimated Quantity**	**Number of Interpreters**	**Calculated Amount (AxB) + (CxD) x E**
Arabic	$250.00	1	$200.00	1	2	$900.00
Armenian	$250.00	1	$200.00	1	2	$900.00
Chinese (including Mandarin and Cantonese)	$250.00	2	$200.00	2	2	$1,800.00
Farsi (Persian)	$250.00	1	$200.00	1	2	$900.00
Filipino (Tagalog)	$250.00	1	$200.00	1	2	$900.00
Japanese	$250.00	1	$200.00	1	2	$900.00
Khmer	$250.00	1	$200.00	1	2	$900.00
Korean	$250.00	1	$200.00	1	2	$900.00
Portuguese	$190.00	1	$160.00	1	2	$700.00
Punjabi (India)	$250.00	1	$200.00	1	2	$900.00
Russian	$250.00	1	$200.00	1	2	$900.00
Spanish	$300.00	10	$300.00	5	2	$9,000.00
Vietnamese	$250.00	1	$200.00	1	2	$900.00
Certified Virtual Simultaneous Interpreter Total (Sum of Column F)						$20,500.00

[1]Rates are for one interpreter, however, due to the length of the events, it is the State's understanding that two interpreters will be required for all simultaneous assignments over one hour.

4. CERTIFIED/QUALIFIED/REGISTERED VIRTUAL CONSECUTIVE INTERPRETER RATES

	A	B	C	D	E
Language	**Full-Day Rate (8 hours)**	**Estimated Quantity**	**Half-Day Rate (4 hours)**	**Estimated Quantity**	**Calculated Amount (AxB) + (CxD)**
Arabic	$250.00	2	$250.00	2	$1,000.00
Armenian	$250.00	2	$250.00	2	$1,000.00
Chinese (including Mandarin and Cantonese)	$250.00	4	$250.00	4	$2,000.00
Farsi (Persian)	$250.00	2	$250.00	2	$1,000.00
Filipino (Tagalog)	$250.00	2	$250.00	2	$1,000.00
Japanese	$250.00	2	$250.00	2	$1,000.00
Khmer	$250.00	2	$250.00	2	$1,000.00
Korean	$250.00	2	$250.00	2	$1,000.00
Portuguese	$160.00	2	$160.00	2	$640.00
Punjabi (India)	$250.00	2	$250.00	2	$1,000.00
Russian	$250.00	2	$250.00	2	$1,000.00
Spanish	$300.00	35	$300.00	20	$16,500.00
Vietnamese	$250.00	2	$250.00	2	$1,000.00
Certified Virtual Consecutive Interpreter Total (Sum of Column E)					$29,140.00

5. DOCUMENT TRANSLATION RATES

	A	B	C	D	E
Language	**24-Hour Turnaround Rate Per Word**	**Estimated Quantity**	**48-Hour Turnaround Rate Per Word**	**Estimated Quantity**	**Calculated Amount (AxB) + (CxD)**
Arabic	$0.10	5000	$0.10	5000	$1,000.00
Armenian	$0.10	5000	$0.10	5000	$1,000.00
Chinese (including Mandarin and Cantonese)	$0.12	5000	$0.11	5000	$1,150.00
Farsi (Persian)	$0.10	5000	$0.10	5000	$1,000.00
Filipino (Tagalog)	$0.10	5000	$0.10	5000	$1,000.00
Japanese	$0.10	5000	$0.10	5000	$1,000.00
Khmer	$0.10	5000	$0.10	5000	$1,000.00
Korean	$0.10	5000	$0.10	5000	$1,000.00
Portuguese	$0.10	5000	$0.10	5000	$1,000.00
Punjabi (India)	$0.10	5000	$0.10	5000	$1,000.00
Russian	$0.10	5000	$0.10	5000	$1,000.00
Spanish	$0.15	20000	$0.15	5000	$3,750.00
Vietnamese	$0.12	5000	$0.11	5000	$1,150.00
				Document Translation Total (Sum of Column E)	**$16,050.00**

COST SHEET SUMMARY- Northern Region

A		B
Table		Amount
1	CERTIFIED/QUALIFIED/REGISTERED IN-PERSON SIMULTANEOUS INTERPRETER RATES **(Sum of Column F)**	$18,500.00
2	CERTIFIED/QUALIFIED/REGISTERED IN-PERSON CONSECUTIVE INTERPRETER RATES **(Sum of Column E)**	$12,750.00
3	CERTIFIED/QUALIFIED/REGISTERED VIRTUAL SIMULTANEOUS INTERPRETER RATES **(Sum of Column F)**	$20,500.00
4	CERTIFIED/QUALIFIED/REGISTERED VIRTUAL CONSECUTIVE INTERPRETER RATES **(Sum of Column E)**	$29,140.00
5	DOCUMENT TRANSLATION RATES **(Sum of Column E)**	$16,050.00
	Total Amount (Sum of Column B)	$96,940.00

NOTE:

- The State will not pay for fees not listed on Exhibit B, Attachment 1, Cost Sheet (i.e., travel, freight, trip, tax, and/or fuel surcharges, etc.).
- Contractor shall be responsible for supplying miscellaneous materials (i.e., grease, lubrications, gloves, etc.) incidental to service, including safety materials needed or required to perform service, at no additional charge to the State.
- Languages not specifically identified on the Cost Sheets may be charged at a rate selected solely by the Contractor but shall not exceed the highest rate on Exhibit B, Attachment 1, Cost Sheet, for the same service, and same timeframe, provided.
- Contractor will provide all labor, materials, tools, and equipment, and shall pay all expenses including, but not limited to, travel, mileage, parking, taxes, insurance, bonds, license and permit fees, and any other costs incidental to providing services.
- Overage Fees may be applied per Exhibit A, Section 10.
    a. Should scheduled appointment last more than 15 minutes longer than the originally scheduled four (4) or eight (8) hour time frame, the supplementary service will be charged as an additional four (4) hour service.
- Cancellation Fees may be applied per Exhibit A, Section 10.
    a. Cancellations made by OAH more than 48 hours prior to the scheduled time will incur no cancellation fee.
    b. Cancellations made by OAH 48 hours or less, but more than, or equal to, 24 hours prior to the time scheduled will incur a charge equal to half of the service charge scheduled for that day.
    c. Cancellations made by OAH less than 24 hours prior to the scheduled time will be charged for the time scheduled for that day.

EXHIBIT D

SPECIAL TERMS AND CONDITIONS

1. STANDARD CONDITIONS OF SERVICE

   A. Contractor will abide by all State and Federal laws in performance of this contract.

   B. The Contractor shall maintain all license(s) required by law for accomplishing any work required with this agreement. In the event any license(s) expire at any time during the term of this agreement, Contractor agrees to provide to the State a copy of the renewed license(s) within thirty (30) days following the expiration date. In the event the Contractor fails to keep in effect at all times all required license(s), the State may, in addition to any other remedies it may have, terminate this agreement upon occurrence of such event.

   C. The Contractor certifies that it has appropriate systems and controls in place to ensure that State funds will not be used in the performance of this Contract for the acquisition, operation or maintenance of computer software in violation of copyright laws.

   D. If signing this contract as a sole proprietor, Contractor certifies that it is not an alien that is ineligible for state and local benefits, as defined in Subtitle B of the Personal Responsibility and Work Opportunity Act (8 U.S.C. § 1601 et seq.).

   E. Pursuant to Public Contract Code section 10295.4, persons or companies identified as the largest tax delinquents by the Franchise Tax Board (FTB) or the California Department of Tax and Fee Administration (CDTFA) are ineligible to enter into any contract with the state for non-IT goods or services. Any contract entered into in violation of section 10295.4 is void and unenforceable.

   F. If contract activities include collection of organic waste, the Contractor must be aware and adhere to Public Resources Code § 42649.1 et. seq. concerning organic waste recycling requirements. Organic waste includes food waste, green waste, landscape and pruning waste, nonhazardous wood waste, and food-soiled paper waste that is mixed in with food waste.

   G. The Contractor's, and any subcontractor's, own data center or cloud computing, where data may be stored, must be physically located in the continental United States. Remote access to data from outside the continental United States is prohibited.

2. EXCISE TAX: The State of California is exempt from Federal Excise Taxes, and no payment will be made for any taxes levied on employees' wages. The State will pay for any applicable State of California or local sales or use taxes on the services rendered or equipment or parts supplied pursuant to this agreement. California may pay any applicable sales or use tax imposed by another state.

3. RIGHT TO TERMINATE

   A. The State reserves the right to cancel all or a portion of the service for any reason, subject to thirty (30) days written notice to the Contractor.

   B. This agreement can be immediately terminated for cause. The term "for cause" means that the Contractor fails to meet the terms, conditions, and/or responsibilities of the contract. In this instance, the contract termination shall be effective as of the date indicated on the State's notification to the Contractor.

4. RESOLUTION OF CONTRACT DISPUTES

   A. In the event of a dispute, Contractor will attempt resolution with the OAH Contract Administrator with a written explanation of the situation. If no resolution is found, Contractor shall file a "Notice of Dispute" with the Department of General Services within ten (10) days of the failed resolution at the following address:

      Attn: Deputy Director and Assistant Chief ALJ
      Department of General Services, OAH
      2349 Gateway Oaks Drive, Suite 200
      Sacramento, CA 95833

   B. Deputy Director and Assistant Chief ALJ or designee shall meet with the Contractor for purposes of resolving the dispute. The decision of the Deputy Director and Assistant Chief ALJ or the designee shall be final. In the event of a dispute, the language contained within this agreement and its attendant Exhibits shall prevail over any other language.

   C. Neither the pendency of a dispute nor its consideration by the Deputy Director and Assistant Chief ALJ will excuse the Contractor from full and timely performance in accordance with the terms of the Agreement.

5. HEALTH AND SAFETY PROVISIONS

   A. Contractor and all subcontractors shall abide by all health and safety mandates issued by federal, state, and local governments and/or public health officers as well as those issued by DGS, and worksite specific mandates. If multiple mandates exist, the Contractor and subcontractors shall abide by the most restrictive mandate. The term "employee", "worker", "state worker" or "state employee" in health and safety mandates includes contractor and subcontractor personnel.

   B. Costs associated with adhering to health and safety mandates are the responsibility of the Contractor. Contractor is responsible for the tracking and compliance of health and safety mandates and may be audited upon request.

6. SUBCONTRACTORS

A. Nothing contained in this Agreement or otherwise, shall create any contractual relationship between OAH and any subcontractors, and no subcontract shall relieve the Contractor of its responsibilities and obligations hereunder. The Contractor agrees to be as fully responsible to OAH for the acts and omissions of its subcontractors and of persons either directly or indirectly employed by the Contractor. The Contractor's obligation to pay its subcontractors is an independent obligation from OAH's obligation to make payments to the Contractor. As a result, OAH shall have no obligation to pay or to enforce the payment of any monies to any subcontractor.

B. Any subcontractors are identified in Exhibit D, Attachment 1.

7. INSURANCE REQUIREMENT

A. General Provisions Applying to All Policies
   1) Coverage Term – Coverage needs to be in force for the complete term of the contract. If insurance expires during the term of the contract, a new certificate must be received by the State at least thirty (30) days prior to the expiration of this insurance. Any new insurance must still comply to the original terms of the contract.
   2) Policy Cancellation or Termination & Notice of Non-Renewal – Contractor is responsible to notify the State within 5 business days of any cancellation, non-renewal or material change that affects required insurance coverage. In the event Contractor fails to keep in effect at all times the specified insurance coverage, the State may, in addition to any other remedies it may have, terminate this Contract upon the occurrence of such event, subject to the provisions of this Contract.
   3) Deductible – Contractor is responsible for any deductible or self-insured retention contained within their insurance program.
   4) Primary Clause – Any required insurance contained in this contract shall be primary, and not excess or contributory, to any other insurance carried by the State.
   5) Insurance Carrier Required Rating – All insurance companies must carry a rating acceptable to the Office of Risk and Insurance Management. If the Contractor is self-insured for a portion or all of its insurance, review of financial information including a letter of credit may be required.
   6) Endorsements – Any required endorsements requested by the State must be physically attached to all requested certificates of insurance and not substituted by referring to such coverage on the certificate of insurance.
   7) Inadequate Insurance – Inadequate or lack of insurance does not negate the Contractor's obligations under the contract.
   8) Subcontractors – If Contractor has identified subcontractors for the work/services identified in the scope of work, the Contractor shall include all subcontractors as insureds under Contractor's insurance or supply evidence of subcontractor's insurance to the State equal to policies, coverages and limits required of Contractor.

B. Commercial General Liability – Contractor and any subcontractors shall maintain general liability on an occurrence form with limits not less than $1,000,000 per occurrence for bodily injury and property damage liability combined. If Commercial General Liability insurance or other form with a general aggregate limit is used, either the general aggregate limits shall apply separately to this project/location, or the general aggregate limit shall be twice the required occurrence limit. If the aggregate applies "per project/location" it shall so state on the certificate. The policy shall include coverage for liabilities arising out of premises, operations, independent contractors, products, completed operations, personal & advertising injury, and liability assumed under an insured contract. This insurance shall apply separately to each insured against whom claim is made or suit is brought subject to the Contractor's limit of liability. **The policy must be endorsed to include the State of California, its officers, agents and employees as additional insured, but only with respect to work performed under the contract. The additional insured endorsement shall be provided with the certificate of insurance.**

C. Automobile Liability – Contractor shall maintain motor vehicle liability with limits not less than $1,000,000 combined single limit per accident. Such insurance shall cover liability arising out of a motor vehicle including owned, hired and non-owned motor vehicles. **The policy must be endorsed to include the State of California, its officers, agents and employees as additional insured, but only with respect to work performed under the contract. The additional insured endorsement shall be provided with the certificate of insurance.**

D. Workers Compensation and Employers Liability – Contractor shall maintain statutory worker's compensation and employer's liability coverage for all its employees who will be engaged in the performance of the Contract. Employer's liability limits of $1,000,000 are required. **The Workers' Compensation policy shall be endorsed with a waiver of subrogation in favor of the State.**

E. Errors and Omissions/Professional Liability- Contractor shall maintain Errors and Omissions/Profession liability with limits of not less than $1,000,000 each incident and $2,000,000 aggregate covering damages caused by negligent, acts or omissions. The policy retro date must be shown on a certificate of insurance and must be before the Contract date, or before the date contract work begins. Insurance must be maintained, and evidence of insurance must be provided for at least five (5) years after completion of the contract of work. If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a retroactive date prior to the contract effective date, the Contractor must purchase "extended reporting" coverage for a minimum of five (5) years after the completion of work.

F. Certificate of Insurance - The Contractor shall furnish a Certificate of Insurance. The Certificate of Insurance will provide the above listed liability coverages and the Certificate Holder shall read

Department of General Services, The Ziggurat
Attn: CSS – 24-209710, OBAS
Mailstop: 508
707 Third Street
West Sacramento, CA 95605

8. RUSSIAN SANCTION ORDERS: On March 4, 2022, Governor Gavin Newsom issued Executive Order (EO) N-6-22 regarding Economic Sanctions against Russia and Russian entities and individuals. “Economic Sanctions” refers to sanctions imposed by the U.S. government in response to Russia’s actions in Ukraine, as well as any sanctions imposed under state law. The EO directs state agencies to terminate contracts with, and to refrain from entering any new contracts with, individuals or entities that are determined to be a target of Economic Sanctions. Accordingly, should the State determine Contractor is a target of Economic Sanctions or is conducting prohibited transactions with sanctioned individuals or entities, that shall be grounds for termination of this agreement. The State shall provide Contractor advance written notice of such termination, allowing Contractor at least 30 calendar days to provide a written response. Termination shall be at the sole discretion of the State.

9. NEWS RELEASES: News releases pertaining to award of, or work performed as a result of, contract may not be made without prior written approval of:

   The Public Information Officer
   707 Third Street, MS 101
   West Sacramento, CA 95605
   Phone: (916) 376-5037
   Email: DGSPublicAffairs@dgs.ca.gov

10. GENAI TECHNOLOGY USE & REPORTING: During the term of the contract, Contractor must notify the State in writing if their services or any work under this contract includes, or makes available, any previously unreported GenAI technology, including GenAI from third parties or subcontractors. Contractor shall immediately complete the GenAI Reporting and Factsheet (STD 1000) to notify the State of any new or previously unreported GenAI technology. At the direction of the State, Contractor shall discontinue the use of any new or previously undisclosed GenAI technology that materially impacts functionality, risk or contract performance, until use of such GenAI technology has been approved by the State. Failure to disclose GenAI use to the State and submit the GenAI Reporting and Factsheet (STD 1000) may be considered a breach of the contract by the State at its sole discretion and the State may consider such failure to disclose GenAI and/or failure to submit the GenAI Reporting and Factsheet (STD 1000) as grounds for the immediate termination of the contract. The State is entitled to seek any and all relief it may be entitled to as a result of such non-disclosure.

    The State reserves the right to amend the contract, without additional cost, to incorporate GenAI Special Provisions into the contract at its sole discretion and/or terminate any contract that presents an unacceptable level of risk to the State.

EXHIBIT E

ADDITIONAL PROVISIONS

1. INTERPRETER/TRANSLATOR RESPONSIBILITIES

Contractor acknowledges that some of the Administrative Hearings, as well as mediations and other proceedings, for which Contractor provides language services are confidential. Any interpreter providing Certified, Registered, or Qualified language services under this Agreement must not disclose to any other person, either during the proceeding or after the proceeding is complete, information about an Administrative Hearing, mediation, or other proceeding that is confidential, except as necessary for Contractor to comply with this Agreement. If any interpreter is not aware of whether a proceeding is confidential, the interpreter shall inquire of the Administrative Law Judge before the proceeding begins or at the beginning of the proceedings. Nor shall any interpreter providing Certified, Registered, or Qualified services under this Agreement allow any other person to hear the interpretation of confidential proceedings while it is taking place. In addition, any interpreter providing Certified, Registered, or Qualified language services under this Agreement shall abide by the following conduct rules set forth in California Rules of Court, Rule 2.890 Professional Conduct for Interpreters:

(a) [Representation of qualifications] An interpreter must accurately and completely represent his or her certifications, training, and relevant experience.

(b) [Complete and accurate interpretation] An interpreter must use his or her best skills and judgment to interpret accurately without embellishing, omitting, or editing. When interpreting for a party, the interpreter must interpret everything that is said during the entire proceedings. When interpreting for a witness, the interpreter must interpret everything that is said during the witness's testimony.

(c) [Impartiality and avoidance of conflicts of interest]

1. Impartiality - An interpreter must be impartial and unbiased and must refrain from conduct that may give an appearance of bias.

2. Disclosure of conflicts - An interpreter must disclose to the judge and to all parties any actual or apparent conflict of interest. Any condition that interferes with the objectivity of an interpreter is a conflict of interest. A conflict may exist if the interpreter is acquainted with or related to any witness or party to the action or if the interpreter has an interest in the outcome of the case.

3. Conduct - An interpreter must not engage in conduct creating the appearance of bias, prejudice, or partiality.

4. Statements - An interpreter must not make statements to any person about the merits of the case until the litigation has concluded.

(d) [Confidentiality of privileged communications] An interpreter must not disclose privileged communications between counsel and client to any person.

(e) [Giving legal advice] An interpreter must not give legal advice to parties and witnesses, nor recommend specific attorneys or law firms.

(f) [Impartial professional relationships] An interpreter must maintain an impartial, professional relationship with all court officers, attorneys, jurors, parties, and witnesses.

(g) [Continuing education and duty to the profession] An interpreter must, through continuing education, maintain and improve his or her interpreting skills and knowledge of procedures used by the courts. An interpreter should seek to elevate the standards of performance of the interpreting profession.

(h) [Assessing and reporting impediments to performance] An interpreter must assess at all times his or her ability to perform interpreting services. If an interpreter has any reservation about his or her ability to satisfy an assignment competently, the interpreter must immediately disclose that reservation to the court or other appropriate authority.

(i) [Duty to report ethical violations] An interpreter must report to the court or other appropriate authority any effort to impede the interpreter's compliance with the law, this rule, or any other official policy governing court interpreting and legal translating.

Rule 2.890 amended and renumbered effective January 1, 2007; adopted as rule 984.4 effective January 1, 1999.

2. COMPUTER SOFTWARE RESPONSIBILITIES

A. Contractor certifies that it has appropriate systems and controls in place to ensure that State funds will not be used in the performance of this Agreement for the acquisition, operation or maintenance of computer software in violation of copyright laws.

EXHIBIT F

DATA PROCESSING AND DATA PROTECTION

This Data Processing and Data Protection exhibit (DPP) is incorporated into the Agreement between the Contracting Agency (State) and the Contractor as identified on the STD 213.

1. **Definitions.** Capitalized terms used herein shall have the meanings set forth below:
   A. **Confidential Information** means any non-public information, whether in written, oral, graphic, electronic or any other form, including without limitation, unpublished financial information, state goals, policies, practices, plans, and projections, and marketing data, business, financial, technical information, user manuals, forecasts, analyses, software and processes, which information is marked or indicated at the time of disclosure or observation as being "Confidential" or "Proprietary," or which would be deemed by a reasonable person to be confidential or proprietary in nature.

   B. **Personal Information** as set forth in Section 1798.3(a) of the California Information Practices Act (Civil Code 1798 et. seq) means any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, their name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual.

   C. **Sensitive Information** means information that is maintained by the State about an individual's: health, genetic or biometric information; race, ethnic origin; religious beliefs/affiliation; philosophical beliefs; political opinion/membership; trade or union membership; criminal record; or sexual preferences/orientation. It is deemed to be sensitive and confidential by the State because it contains information that may be exempt by statute, regulation, or policy from access by the general public as public information.

   D. **State Data** means all information and data owned by the State, and submitted to, processed by, or stored by Contractor and includes, but is not limited to, all data/information that originated with the State, all data/information provided by the State, and data/information generated, manipulated, produced, reported by or otherwise emanating from or by applications run by the State in order to obtain the Services. State Data includes Personal Information, Sensitive Information, and any and all Confidential Information.

2. **Use of State Data.**

All State Data submitted by the State to Contractor under this Agreement, will remain property of the State. State Data will not be used by Contractor other than in connection with the provision of the contracted services or as required by law. State Data will not be (1) disclosed, sold, assigned, leased or otherwise provided access to third parties by Contractor, or (2) commercially exploited by or on behalf of Contractor, its employees or agents. All State Data made available to the Contractor in order to carry out this Agreement, or which become available to the Contractor under this Agreement, shall be protected by the Contractor from unauthorized use and disclosure, at minimum, by use of the same confidentiality requirements

applicable to or required by the State. All State Data must be stored in a physically and logically secure environment that protects it from unauthorized access, modification, theft, misuse, and destruction.

3. Data Protection.

In addition to the confidentiality obligations under this Agreement, Contractor agrees to limit its use of any Personal and Sensitive Information obtained under this Agreement and to protect such information in accordance with this DPP.

A. Security Program. Contractor will implement and maintain a comprehensive written information security program designed to protect Personal Information, Sensitive Information or other information deemed "Confidential" under this Agreement from unauthorized access, use, modification, disclosure or destruction. Contractor shall certify compliance with the most recent published version of NIST Special Publications 800-53, the California Information Practices Act (Civil Code sections 1798 et seq.), and the privacy provisions of the Federal Privacy Act of 1974.

As part of its information security program, Contractor will limit access to Personal Information, Sensitive Information, or otherwise Confidential Information to the minimum number of Contractor's employees, agents, subcontractors, and other persons who require such access in order to provide services to the State (collectively, Personnel). Contractor shall provide those Personnel who have access to Personal, Sensitive or other Confidential Information with appropriate training on an annual basis and shall provide certification of such training within 5-days of DGS ISO's request. Contractor shall retain training certification for DGS inspection for a period of 3-years after expiration or termination of the Agreement.

B. Use of Personal and Sensitive Information. Contractor will collect, record, organize, structure, alter, access, disclose, copy, transfer, store, delete, combine, restrict, adapt, retrieve, consult, destroy, dispose of or otherwise use Personal Information and Sensitive Information ("Process") only to provide the services described in this Agreement or as otherwise directed in writing by the State unless otherwise required to comply with applicable law. If Contractor is required by applicable law to Process Personal or Sensitive Information beyond the scope of the services, Contractor will notify the State in writing of the legal requirement before Processing unless the notification is prohibited by law.

C. Encryption. Information that is Personal, Sensitive or otherwise Confidential Information shall be encrypted in accordance with California State Administrative Manual 5350.1 and California Statewide Information Management Manual 5305-A.

D. Return of Information. Contractor will return or render permanently unreadable and unrecoverable all State Data at the end of this Agreement or upon the State's written request unless Personal Information or Sensitive Information must be retained by Contractor to comply with applicable laws. Erasure or destruction of all State Data in Contractor's possession shall be in accordance with the Department of General Services' (DGS) standard for data destruction, which DGS shall provide to Contractor. Contractor shall provide certification of destruction to DGS's Information Security Office (ISO).

E. Security Incidents. Contractor agrees to promptly, and in any event within 24 hours of discovery, notify the State in writing of any unauthorized access, use, modification, disclosure or destruction of Personal, Sensitive or otherwise Confidential Information under this Agreement ("**Security Incident**"). Notice shall be sent to the DGS Chief Information Security Officer. Contractor's notification shall identify: (i) the nature of the Security Incident; (ii) data accessed, used or disclosed; (iii) person(s) who accessed, used, disclosed and/or received data (if known); (iv) actions Contractor has taken or will take to quarantine and mitigate the Security Incident; and (v) corrective actions Contractor has taken or will take to prevent future Security Incidents.

Contractor will take all necessary steps to mitigate the harm to the State and/or individuals impacted by the Security Incident. Contractor will cooperate with DGS ISO in the investigation and remediation efforts and shall respond to DGS ISO requests within 24-hours. The Chief Information Security Officer, or designee, shall determine whether notification to the individuals whose data has been lost or breached is appropriate. If Personal or Sensitive Information of any California resident was, or is reasonably believed, to have been acquired by an unauthorized person as a result of a security breach of such system that is not due to the fault of the State, or any person or entity under the control of the State, Contractor shall bear any and all costs associated with the State's notification obligations and other obligations set forth in Civil Code Section 1798.29 (d), as well as the cost of credit monitoring, subject to the dollar limitation, if any, agreed to by the State and Contractor in the applicable Statement of Work. These costs may include, but are not limited to staff time, material costs, postage, media announcements, and other identifiable costs associated with the security breach of such Personal or Sensitive Information.

F. Investigation. Contractor shall investigate the Security Incident and shall share the report of the investigation with the State. The State and/or its authorized agents shall have the right to lead (if required by law) or participate in the investigation. Contractor shall cooperate fully with the State, its agents and law enforcement.

G. Cooperation; Audit. Contractor will provide relevant information and reasonable assistance to the State to demonstrate Contractor's compliance with its obligations under the Agreement and cooperate with reasonable assessments, including onsite reviews, conducted by regulators or the State, at no cost to the State. After any significant data loss or Security Incident, Contractor will, at its expense, have an independent, industry-recognized, State-approved third party perform an information security audit. The audit results shall be shared with the State within seven (7) days of Contractor's receipt of such results. Upon Contractor receiving the results of the audit, Contractor will provide the State with written evidence of planned remediation within thirty (30) days and promptly modify its security measures in order to meet its obligations under this Contract.

H. Public Records Requests and Data Subject Request. Contractor will assist the State with the State's statutory obligation to respond to a Public Records Access request (Government Code section 6250 et. seq) or a data subject's request to access, correct, delete or exercise any other right related to their data under applicable law.

I. Subcontracting. Contractor will not disclose Personal Information, Sensitive Information, or otherwise Confidential Information or allow access to such information to any third party without the State's prior written consent; provided, however, that

Contractor may Disclose Personal Information, Sensitive Information, or otherwise Confidential Information to its affiliates and subcontractors for purposes of providing the services to the State, subject to the following conditions: (a) Contractor receives prior written consent to subcontract and the subcontracting is justified and complies with the conditions in the State Contracting Manual; (b) Contractor will enter into a written agreement with any third party that includes security, privacy and confidentiality provisions at least as restrictive as this Agreement; and (c) Contractor will be liable for all actions by such third parties related to the use, processing and/or disclosure of Personal, Sensitive Information, or otherwise Confidential Information.

I. Background Checks: If Contractor will receive federal tax information or personal health information from the State under this Agreement, Contractor shall conduct a background check for all Contractor personnel who will Process such information. Contractor shall retain personnel background check documentation for a period of three (3) years after the contract ends.

J. Payment Card Data. If Contractor stores, process, and/or transmit the State's customer payment card data, Contractor must provide evidence of compliance with Payment Card Industry (PCI) Data Security Standards. If Contractor develops payment applications that store, process or transmit cardholder data and/or sensitive authentication data as part of authorization or settlement, contractor must provide evidence of compliance with Payment Application Data Security Standard (PA-DSS).

4. Survival.

The obligations of Contractor, its legal representatives, successors, and/or assignees, under this DPP will continue for so long as Contractor continues to have access to Personal, Sensitive Information, or otherwise Confidential Information, even if all agreements between Contractor and the State have expired or have been terminated.

EXHIBIT G

Additional Provisions for Specific OAH Case Types

Certain governmental agencies require OAH to enter into agreements called Business Associate Agreements ("BAAs"), which affect the way confidential or protected information is created, received, maintained, transmitted, used, disclosed and/or disposed. These BAAs require OAH subcontractors be bound to the same terms and conditions as OAH. Copies of these BAAs are incorporated and included with this Agreement as Attachments G-1 through G-4 to this Exhibit.

Contractor agrees to the same BAA terms and conditions as OAH when providing services for cases involving these agencies. Contractor's failure to adhere to the terms and conditions of the below BAAs may be considered a material breach and may result in termination of this Agreement. If subcontracting, Contractor must require the subcontractor(s) to agree to the terms and conditions in the below BAAs.

Contractor shall immediately notify the OAH Contract Administrator upon discovery of a breach. If the cause of a breach of confidential or protected information is attributable to Contractor or its subcontractors, the governmental agency or OAH may require Contractor to notify individuals of the breach when notification is required under state or federal law. Contractor shall pay any costs of such notifications, as well as any costs associated with the breach.

If any governmental agency and OAH amend the below listed BAAs for compliance with state or federal law, the updated BAAs will be added to this contract by a formal amendment.

Attachment No.:	G-1
Agency Name:	Department of Developmental Services (DDS)
Case Type:	• Lanterman Act – disputes between service agencies and applicants for or recipients of regional center services ages three years and up (Welf. & Inst. Code, § 4700 et seq.). • Early Start – disputes between service agencies and applicants for or recipients of regional center services ages birth to three years (34 C.F.R. §§ 303.431 - 303.449). • Residential care facility appeals (Cal. Code Regs., tit. 17, § 56061). • Family Cost Participation Program appeals (Welf. & Inst. Code, § 4783). • Formal audit appeal hearings (Cal. Code Regs., tit. 17, § 50700 et seq.). • Appeals from denials of criminal exemptions (Welf. & Inst. Code, § 4689.6). • Family Home Agency (FHA) appeals (Cal. Code Regs., tit. 17, § 56096), and • Interagency Dispute Resolution for regional centers and generic agencies (Welf. & Inst. Code, §§ 4659.5 to 4659.8).
Document Name:	Statement of Assurances for Protection of Protected Health Information (Revised 12/2017) – Health Insurance Portability and Accountability Act (HIPAA); Health Information Technology for Economic and Clinical Health (HITECH)

Attachment No.:	G-2
Agency Name:	California Department of Corrections and Rehabilitation
Case Type:	• Involuntary medication of prisoners (Pen. Code, § 2602 – formerly known as the *Keyhea* injunction). • Appointment of a surrogate decision maker to make medical care decisions on behalf of an inmate patient who is not competent to make such decisions (Pen. Code, § 2604)
Document Name:	Business Associate Agreement (HIPAA)

Attachment No.:	G-3
Agency Name:	California Department of Corrections and Rehabilitation California Correctional Health Care Services Professional Practices Executive Committee
Case Type:	Privileges of a licensed practitioner (Bus. & Prof. Code, § 809 et seq.)
Document Name:	HIPAA Business Associate Agreement (Standard Risk)

Attachment No.:	G-4
Agency Name:	Department of State Hospitals
Case Type:	Involuntary medication of patients housed at state hospitals (Pen. Code, § 1370)
Document Name:	Confidentiality and Information Security Provisions

EXHIBIT G, ATTACHMENT G-1

Department of Development Services Cases

Case Type and Legal Authority
Lanterman Act – Disputes between service agencies and applicants for, or recipients of, regional center services for children ages three years and up (Welf. & Inst. Code, § 4700 et seq.)
Early Start– disputes between service agencies and applicants for or recipients of regional center services for children ages birth to three years (34 C.F.R. §§ 303.431 - 303.449)
Residential care facility appeals (Cal. Code Regs., tit. 17, § 56061)
Family Cost Participation Program appeals (Welf. & Inst. Code, § 4783)
Formal audit appeal hearings (Cal. Code Regs., tit. 17, § 50700 et seq.)
Appeals from denials of criminal exemptions (Welf. & Inst. Code, § 4689.6)
Family Home Agency (FHA) appeals (Cal. Code Regs., tit. 17, § 56096)
Interagency Dispute Resolution for regional centers and generic agencies (Welf. & Inst. Code, §§ 4659.5 to 4659.8)

Statement of Assurances for Protection of Protected Health Information

Health Insurance Portability and Accountability Act (HIPAA)
Health Information Technology for Economic and Clinical Health (HITECH)
Revised 12/2017

1. Background

The terms of this Agreement are intended to create a business associate relationship between the contracting parties (collectively, "Contractor" and "DDS") as required under the Health Insurance Portability Accountability Act ("HIPAA"), codified in Title 42 of the United States Code, Section 1320d *et seq*. and its implementing law and regulations such as the Health Information Technology for Economic and Clinical Health Act of 2009, (Public Law 111-005, Title XIII, Subtitle D, 42 U.S.C. 17921 Section 13400 et seq.,) ("HITECH Act"), and Title 45 of the Code of Federal Regulations ("CFR") Parts 160 and 164 ("HIPAA Regulations").

Since a business associate relationship is created by this Agreement and protected health information ("PHI"), as defined in Section 3 herein, may be exchanged, created, received, maintained, used and/or disclosed to Contractor, Contractor agrees to comply with all applicable requirements of HIPAA, HIPAA Regulations, and the HITECH Act which pertain to the privacy and security of PHI.

In addition, HIPAA's preemption exception under Title 45 of the CFR Section 160.203 requires state law to apply if state law is more stringent in protecting PHI. Accordingly, the intent of the parties is that Contractor shall comply with applicable California law

governing the exchange, creation, dissemination, maintenance, use or disclosure of PHI that exceeds the requirements of HIPAA, HIPAA Regulations, and the HITECH Act.

2. Recitals

A. DDS wishes to disclose to Contractor and/or wishes for the Contractor to receive certain information pursuant to the terms of this Agreement, some of which may constitute PHI.

B. As set forth in this Agreement Contractor is the "Business Associate", as defined in Section 3 herein, of DDS that provides services, arranges, performs or assists in the performance of functions or activities on behalf of DDS and creates, receives, maintains, transmits, uses or discloses PHI.

C. DDS and Contractor desire to protect the privacy and provide the security of PHI created, received, maintained, transmitted, used, or disclosed pursuant to this Agreement, in compliance with HIPAA, HIPAA Regulations, the HITECH Act, and any more stringent applicable state law protecting PHI.

Now, therefore, the parties agree as follows:

3. Definitions

A. ***Accounting –*** "Accounting" means Contractor's accounting of PHI disclosures to an individual upon his or her request in accordance with 45 CFR § 164.528, subject to the exceptions listed therein. As stated in 45 CFR § 164.528(b) an accounting includes the date of disclosure, the name of the entity or person who received the PHI and, if known, the address of such entity or person, a brief description of the PHI disclosed, and a brief statement of the purpose of disclosure or copy of a written request for disclosure by the Secretary, as defined herein, or by an entity or person permitted under 45 CFR § 164.512.

B. ***Breach or Breaches*** – "Breach" or "Breaches" have the same meaning of the term "breach" defined under 45 CFR § 164.402, which is the acquisition, access, use or disclosure of PHI in a manner not permitted under Title 45 of the CFR Part 164, Subpart E, that compromises the security or privacy of PHI, subject to the breach exclusions listed therein.

C. ***Business Associate*** – "Business Associate" has the same meaning of the term "business associate" defined in 45 CFR § 160.103, which means an entity or person on behalf of a covered entity who creates, receives, maintains or transmits PHI by conducting services including legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, financial services, claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, patient safety activities benefit management, practice management and/or repricing. "Business associate" also refers to Contractor who is a party to this Agreement.

D. ***Covered Entity*** – "Covered Entity" has the same meaning of the term "covered entity" defined in 45 CFR § 160.103, which means a health plan, health

clearinghouse or healthcare provider. Covered entity also refers to DDS who is a party to this Agreement.

E. ***Designated record set –*** "Designated record set" has the same meaning of the term "designated record set" defined in 45 CFR § 164.501, which is a group of records that contains PHI and is maintained by or for a covered entity. The designated record set includes medical records and billing records, enrollment, payment, claims adjudication and case/medical management record systems, and/or records used, in whole or part, to make decisions about individuals.

F. ***Disclosure –*** "Disclosure" has the same meaning of the term "disclosure" defined in 45 CFR § 160.103, which is the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

G. ***Discovery –*** "Discovery" has the same meaning of "Breaches treated as discovered" under 45 CFR § 164.410. Under Section 164.410, a breach shall be treated as discovered by a business associate on the first day on which such breach is known, or by exercising reasonable diligence would have been known by the business associate, including its employees or agents.

H. ***Electronic PHI –*** "Electronic PHI" is protected health information in an electronic form. (See P. below for definition of PHI.)

I. ***Encryption –*** "Encryption" has the same meaning of the term "encryption" defined in 45 CFR § 164.304, which is the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

J. ***Harmful effect –*** "Harmful effect" means a negative effect of using or disclosing PHI known to the covered entity or business associate that would violate HIPAA, HIPAA Regulations, the HITECH Act, as set forth in 45 CFR § 164.530(f), or any more stringent applicable state law protecting PHI.

K. ***Health care operations –*** "Health care operations" has the same meaning of the term "health care operations" defined in 45 CFR § 164.501. Under Section 164.501, health care operations include conducting quality assessment and improvement activities, outcomes evaluation, development of clinical guidelines, patient safety activities, population-based activities relating to improving health, protocol development, case management and care coordination, reviewing competence and qualifications of health care professionals not involving treatment, evaluating provider/vendor performance, conducting training programs for students, trainees or practitioners in the area of health care to improve skills, training of non-health care professionals, accreditation, certification, licensing or credentialing activities, underwriting and enrollment relating to creation, renewal or replacement of health insurance or benefits, medical review, legal services, auditing functions, business planning and development, business management and general administrative activities such as implementation and compliance with HIPAA, HIPAA Regulations, and the HITECH Act, customer service, resolution of internal grievances, the creation of de-identified health information or a limited

data set, and/or fundraising for the benefit of the business associate.

L. ***Individual or Individuals –*** "Individual" or "Individuals" have the same meaning of the term "individual" defined in 45 CFR § 160.103, which is the person who is the subject of PHI.

M. ***Limited Data Set*** – "Limited Data Set" has the same meaning of the term "limited data set" defined in 45 CFR § 164.514(e)(2). Under Section 164.514(e)(2), limited data set excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individuals: (1) names; (2) addresses, other than town or city, state and zip code; (3) telephone numbers; (4) fax numbers; (5) email addresses; (6) social security numbers; (7) medical record numbers; (8) health plan beneficiary numbers; (9) account numbers; (10) certificate/license numbers; (11) vehicle identifiers and serial numbers, including license plate numbers; (12) device identifiers and serial numbers; (13) URLs; (14) IP address numbers; (15) biometric identifiers, including finger and voice prints; and (16) full face photographic images and any comparable images.

N. ***Minimum necessary*** – "Minimum necessary" means the "minimum necessary" standard set forth in 45 CFR § 164.502, which requires covered entities and business associates to make reasonable efforts to limit the use or disclosure of PHI to accomplish the intended purpose of the use, disclosure or request, subject to the exceptions set forth therein.

O. ***Notice of Privacy Practices –*** "Notice of Privacy Practices" means the required notice under 45 CFR § 164.520 provided to individuals by a covered entity regarding the use and disclosure of PHI that may be made by the covered entity, and the individual's rights and covered entity's legal duties with respect to PHI.

P. ***PHI or protected health information –*** "PHI" or "protected health information" have the same meaning of the term "individually identifiable health information" as defined in 45 CFR § 160.103. Under Section 160.103 individual identifiable health information is information that is created or received by a covered entity or business associate that relates to the past, present, or future physical or mental health of an individual; or the past, present, or future payment for the provision of health care to the individual. In addition, the information must identify the individual or there must be a reasonable basis to believe the information may be used to identify the individual.

Q. ***Required by law –*** "Required by law" has the same meaning of the term "required by law" defined in 45 CFR § 164.103, which is a mandate contained in law that compels an entity to make a use or disclosure of PHI and that is enforceable in a court of law.

R. ***Safeguards*** – "Safeguards" referenced herein collectively means the required "administrative safeguards" defined in 45 CFR § 164.308, "physical safeguards" defined in 45 CFR § 164.310, and "technical safeguards" defined in 45 CFR § 164.312.
   1) Under 45 CFR § 164.308 "administrative safeguards" is the implementation of policies and procedures to prevent, detect, contain and correct security

violations.

2) Under 45 CFR § 164.310 "physical safeguards" is the implementation of policies and procedures to limit physical access to electronic information systems and the facility or facilities in which PHI is maintained, while ensuring proper authorized access to PHI.
3) Under 45 CFR § 164.312 "technical safeguards" is the implementation of policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights specified in 45 CFR § 164.308(a)(4).

S. ***Secretary –*** "Secretary" means the Secretary of the United States Department of Health and Human Services.

T. ***Security Incident –*** "Security Incident" has the same meaning of the term "security incident" defined in 45 CFR § 164.304, which is the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.

U. ***Subcontractor or Agent –*** "Subcontractor" or "Agent" have the same meaning of the term "subcontractor" defined in 45 CFR § 164.304, which is a person to whom a business associate delegates a function, activity or service, other than in the capacity of a member of the workforce of such business associate.

V. ***Unsecured PHI*** – "Unsecured PHI" has the same meaning of "unsecured protected health information" defined in 45 CFR § 164.402, and it is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology and methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.

W. ***Use or usage –*** **"**Use" or "usage" have the same meaning of the term "use" defined in 45 CFR § 160.103, which is the sharing, employment, application, utilization, examination, or analysis of PHI within an entity that maintains such information.

4. Permitted Uses and Disclosures of PHI by Business Associate

A. ***Usage Permitted by This Agreement and HIPAA***. Contractor may use or disclose PHI only to perform functions, activities or services for, or on behalf of the DDS as specified in this Agreement, provided that such use or disclosure does not violate HIPAA, HIPAA Regulations, the HITECH Act, and any more stringent applicable state law protecting PHI. The use and disclosure of PHI may not be more expansive than applicable to DDS as the "Covered Entity" under 45 CFR Part 164. (45 CFR § 164.504(e)(2)(i)).

B. ***Usage for Legal, Management and Administrative***. In accordance with 45 CFR § 164.504(e)(4), Contractor may disclose PHI if necessary for the legal, management, or administrative purposes of Contractor. In disclosing PHI, Contractor's disclosure must be required by law, or the Contractor must obtain reasonable assurances from the person to whom the information is disclosed that

it will remain confidential and 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 Contractor of any instances of which it is aware in which the confidentiality of the information has been breached.

C. ***Minimum Necessary***. Contractor shall comply with the requirements under 45 CFR § 164.502(b) to only request, use, and disclose the minimum PHI necessary to accomplish the intended purpose of the request, use or disclosure.

D. ***Access***. Contractor shall provide access, at the request of DDS, and in the time and manner designated by DDS, to PHI in a designated record set to DDS or, as directed by DDS, to an individual in order to meet the requirements of 45 CFR § 164.524 and 45 CFR § 164.504(e)(2)(ii)(E) regarding an individual's right to access PHI.

1) If Contractor maintains electronic PHI, and an individual requests a copy of his or her PHI in an electronic format, Contractor shall provide such information in an electronic format to enable DDS to fulfill its obligations under the HITECH Act, including but not limited to 42 USC § 17935(e).

E. ***Nondisclosure***. In accordance with 45 CFR § 164.504(e)(2)(ii)(A), Contractor shall not use or further disclose PHI other than as permitted or required by this Agreement, or as required by law.

F. ***Amendments***. In accordance with 45 CFR § 164.504(e)(2)(ii)(F) and 45 CFR § 164.526(a)(2), Contractor shall make any amendment(s) to PHI in a designated record set that DDS directs or agrees to and in the time and manner designated by DDS, or at the request of an individual. If an individual makes such request directly to the Contractor, Contractor will forward to DDS within five (5) business days of receipt. Contractor shall ensure the amendment/s are incorporated into the PHI in accordance with 45 CFR § 164.526.

G. **Accounting**.

1) Except as provided in Section 4.G.2 herein, Contractor shall document and track disclosures of PHI that it creates, receives, maintains or transmits on behalf of DDS to establish an accounting. The accounting of disclosures shall include: (1) the date of disclosure; (2) the name of the entity or person who received the PHI and, if known, the address of such entity or person; (3) a brief description of the PHI disclosed; and (4) a brief statement describing the reason for the required or permitted disclosure (e.g., pursuant to a court order), or a copy of the written request if applicable as required under 45 CFR § 164.528(b)(2).

2) Contractor is not required to document and track disclosures of PHI that it creates, receives, maintains or transmits on behalf of DDS only for the following reasons in accordance with 45 CFR § 164.528(a)(1):

a. Disclosures made for treatment, payment and healthcare operations;
b. Disclosures made to the individual about themselves;
c. Disclosures resulting from or incident to otherwise permitting disclosure in 45 CFR § 164.502;
d. Disclosures made pursuant to a valid HIPAA authorization under 45 CFR § 164.508(c);
e. Disclosures made for the Contractor's director, or to persons involved in the individual's care or for related purposes as provided in 45 CFR § 164.510;
f. Disclosures made pursuant to national security or intelligence purposes as provided in 45 CFR § 164.512 (k)(2);
g. Disclosures made to correctional institutions or law enforcement as provided in 45 CFR § 164.512(k)(5); and
h. Disclosures that are part of a limited data set.

3) Contractor shall provide an accounting of disclosures of PHI to DDS or an individual for the six years prior to the date of the request, in accordance with 45 CFR § 164.528 (a)(1), subject to the exceptions listed therein. Contractor shall respond in writing to a request for accounting of disclosures within thirty (30) calendar days of receipt of the request by producing the accounting of disclosures or verifying there were no disclosures.

5. Uses and Disclosures Not Provided for by this Agreement

A. ***Mitigation***. In accordance with 45 CFR § 164.530 (f), Contractor shall mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of PHI in violation of the requirements of this Agreement.

B. ***Requests to Restrict PHI. Contractor shall not disclose PHI about an individual to a health plan for payment or health care operations purposes if 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 USC § 17935(a) and 45 CFR 164.522(a).***

C. ***No Remuneration Without Written Consent. In accordance with 42 USC § 17935(d)(1) Contractor shall not directly or indirectly receive remuneration in exchange for PHI, except with the prior written consent of DDS and a valid HIPAA authorization under 45 CFR § 164.508.***

6. Safeguarding Protected Health Information

A. In accordance with 45 CFR § 164.504(e)(2)(ii)(B) and 45 CFR Part 164, Subpart C, Contractor shall use appropriate safeguards to prevent use or disclosure of PHI, except as provided in this Agreement or as required by law.

B. In accordance with 45 CFR Part 164, Subpart C and 45 CFR § 164.314(a)(2)(i)(A) & (B), Contractor shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI, including electronic PHI, it creates, receives, maintains, or transmits in an electronic format on behalf of DDS to prevent unauthorized access, viewing, use, disclosure or breach of PHI, other than as provided for by this Agreement or required by law.

C. Contractor shall develop and maintain a written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of Contractor's operations and the nature and scope of its activities, and which incorporates the requirements of Section 7, Security, below.

D. ***Privacy Officer.*** Contractor shall designate a Privacy Officer who shall: (1) develop policies and procedures on PHI that comply with this Agreement, HIPAA, HIPAA Regulations, the HITECH Act, and any more stringent applicable state law protecting PHI; (2) receive complaints/notices pertaining to breaches, and process those complaints/notices in accordance with Section 10, herein; and (3) be the point of contact for communication on privacy matters with DDS. Contractor shall notify DDS's privacy and security officers of the individual designated as Privacy Officer and his/her appropriate contact information (including telephone, work address and email) upon execution of this Agreement, and within 10 calendar days of any changes.

7. Security

A. Contractor shall ensure the security of all computerized data systems containing PHI in compliance with HIPAA, HIPAA Regulations and the HITECH Act, and in accordance with 45 CFR § 164.502(e)(1). These steps shall include, at a minimum, but not be limited to:

1) Ensuring appropriate security levels to maintain the confidentiality, integrity and availability of PHI and electronic PHI in accordance with 45 CFR Part 164, Subpart C;

2) Protecting against any reasonably anticipated threats or hazards to the security or integrity of PHI and electronic PHI in accordance with 45 CFR 164.306(a)(2);

3) Protecting against any reasonably anticipated uses or disclosures of PHI and electronic PHI that are not permitted or required under 45 CFR Part 164, Subpart E, in accordance with 45 CFR 164.306(a)(3);

4) Requiring encryption of electronic PHI that is confidential, sensitive, or personal when it is stored or transmitted using portable computing devices (including, but not limited to, tablets, smartphones, laptops and notebook computers, electronic tapes) and/or portable electronic storage media (e.g.,

CD, DVD, flash drives, etc.); and

5) Designating a Security Officer pursuant to 45 CFR § 164.308 to oversee Contractor's data security program. The Security Officer shall be responsible for carrying out the requirements of this Section and to be the point of contact for communicating on security matters with DDS. Contractor shall notify DDS's privacy and security officers of the individual designated as Security Officer and his/her appropriate contact information (including telephone, work address and email) upon execution of this Agreement, and within 10 calendar days of any changes.

8. Agents and Subcontractors

A. Contractor shall require any of its agents, including subcontractors, that create, receive, maintain, or transmit PHI and/or electronic PHI on behalf of Contractor pursuant to its Agreement with DDS, to agree to the same restrictions, safeguards, and conditions that apply to Contractor herein with respect to such information. (45 CFR §§ 164.502, 164.504, 164.506, 164.314(a)(2)(i)(B)).

B. Contractor's agents and subcontractors who create, receive, maintain, or transmit PHI and/or electronic PHI on behalf of Contractor are business associates of Contractor and are directly liable under HIPAA, HIPAA Regulations and the HITECH Act for any breach they commit. As such, Contractor's agents and subcontractors who create, receive, maintain, or transmit PHI and/or electronic PHI are subject to civil and, in some cases, criminal penalties for making uses and disclosures of PHI that are not authorized by contract or required by law. Contractor's agents and subcontractors who create, receive, maintain, or transmit electronic PHI, are also directly liable and subject to civil penalties for failing to safeguard electronic PHI in accordance with HIPAA, HIPAA Regulations, and the HITECH Act.

9. Records available to the State and Secretary and Compliance Reviews

A. In accordance with 45 CFR § 164.504(e)(ii)(2)(I), Contractor shall make its internal practices, books and records relating to the use and disclosure of PHI received from DDS, or created or received by Contractor on behalf of DDS, available to DDS or to the Secretary for purposes of investigating or auditing DDS's compliance with the requirements of HIPAA, HIPAA Regulations, and the HITECH Act, in the time and manner designated by DDS or the Secretary.

B. In accordance with 45 CFR § 160.310, Contractor shall cooperate with the compliance and investigation reviews conducted by the Secretary. PHI access to the Secretary must be provided during Contractor's normal business hours, however, upon exigent circumstances access at any time must be granted. Upon the Secretary's compliance or investigation review, if PHI is unavailable to Contractor and in possession of a subcontractor or agent, it must certify efforts to obtain the information to the Secretary.

10. Breach Procedure

A. ***Discovery of Breach***. Contractor shall notify DDS ***within 72 hours by telephone call plus email*** upon the discovery of a breach compromising the security and/or privacy of PHI, or upon a reasonable belief such breach has occurred, as required at 45 CFR §164.410. Notification shall be provided to the DDS Privacy Officer and the DDS Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves electronic PHI, notification shall be provided by calling the DDS Service Desk. Upon discovery of such breach or reasonable belief of such breach, Contractor shall immediately:

1) Take prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and
2) Commence an investigation.

Content of Notification: In accordance with 45 CFR §§ 164.404(c),164.410, within 72 hours of discovery of such breach or reasonable belief such breach occurred, Contractor shall include the following information in the notification to the DDS Privacy Officer and the DDS Information Security Officer to the extent known:

1) Identification of each individual whose unsecured PHI or confidential information has been, or is reasonably believed to have been accessed, acquired, used, disclosed, or breached;
2) A description of the probable causes of the improper use or disclosure;
3) What data elements were involved and the extent of the data involved in the breach;
4) A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed PHI or electronic PHI;
5) A description and date/s of where the PHI is believed to have been improperly utilized;
6) A description of the steps that an individual may take to protect him/her from the breach; and
7) A description of what Contractor is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.

B. ***Written Report***. In accordance with 45 CFR § 164.504(e)(2)(ii)(C) and 45 CFR § 164.410, Contractor shall provide a written report of the investigation to the DDS Privacy Officer and the DDS Information Security Officer within thirty (30) calendar days of the discovery of the breach or unauthorized use or disclosure.

C. ***Notification of Individuals.*** Contractor or Contractor's subcontractor or agent shall notify individuals whose unsecured PHI has been or is reasonably believed by Contractor to have been accessed, acquired, used, transmitted, or disclosed

as a result of the breach as required under 45 CFR § 164.404. Notification shall be provided without unreasonable delay as required by 42 USC § 17932(d), and within 30 calendar dates. Contractor, or Contractor's subcontractor or agent, shall pay any costs of such notifications, as well as any costs associated with the breach. The DDS Privacy Officer and the DDS Information Security Officer shall approve the time, manner and content of any such notifications.

D. ***Responsibility for Reporting Breaches Involving Less Than 500 Individuals.*** If the cause of breach of PHI or electronic PHI is attributable to the Contractor, or its subcontractors or agents, Contractor is responsible for all required reporting of the breach as specified in 42 USC § 17932 and 45 CFR Part 164, Subpart D. The breach reporting requirements of this paragraph are in addition to the reporting requirements set forth in subsection 10(A-C) above.

E. ***Responsibility for Reporting Breaches Involving 500 or More Individuals.*** If a breach of unsecured PHI involves 500 or more residents of the State of California or its jurisdiction, Contractor and DDS shall jointly notify the Secretary of the breach immediately upon discovery of the breach and prominent media outlets serving the State of California or its jurisdiction in accordance with 42 USC § 17932 and 45 CFR §§ 164.406, 164.408. The breach reporting requirements of this paragraph are in addition to the reporting requirements set forth in subsection 10(A-C) above.

F. ***DDS Contact Information.*** Contractor shall direct communications to the following DDS staff. DDS 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 Agreement.

DDS **Privacy Officer**	DDS **Information Security Officer**
Privacy Officer **REDACTED** **REDACTED**	Information Security Officer **REDACTED** **REDACTED**

11. Term and Termination

A. ***Term.*** The term of this Agreement shall terminate when this contract expires or when all of the PHI provided by the DDS to Contractor, or created or received by Contractor on behalf of the DDS, in any format, is returned to the DDS and any associated storage media is destroyed, whichever is later.

B. ***Termination for Cause.*** Upon DDS's knowledge of a pattern of activity or practice by Contractor that constitutes a material violation of this Agreement by Contractor, DDS shall:

1) Provide Contractor with a written notice of the existence of such material violation and a 30-day notice to cure the breach.
2) If Contractor fails to cure such material violation within 30 days, DDS may immediately terminate this contract on written notice. DDS shall report the violation to the HHS Secretary if such cure is not possible.

C. **Judicial or Administrative Proceeding**

DDS may terminate this Agreement in accordance with the terms and conditions of this Agreement as written herein above if: (1) Contractor is found guilty in a criminal proceeding for a violation of the HIPAA, HIPAA Regulations, or the HITECH Act; or (2) a finding or stipulation that the Contractor has violated a privacy or security standard or requirement of HIPAA, HIPAA Regulations , the HITECH Act, or any more stringent applicable state law protecting PHI in an administrative or civil proceeding in which Contractor is a party.

D. **Effect of Termination or Nonrenewal**

1) In accordance with 45 CFR § 164.504(e)(2)(ii)(J), upon termination of this Agreement or nonrenewal of this Agreement, Contractor shall, if reasonably feasible, return or destroy all PHI and/or electronic PHI received from DDS, or created or received by Contractor on behalf of the DDS. Contractor shall, if reasonably feasible, require that any PHI and/or electronic PHI in possession of subcontractors or agents is returned or destroyed and that no copies of such information is retained.
2) In the event Contractor determines that returning or destroying the PHI and/or electronic PHI is reasonably infeasible, Contractor shall notify DDS about the conditions that make return or destruction not feasible. If DDS agrees that the return or destruction of PHI and/or electronic PHI is not feasible, Contractor shall extend the protections of this Agreement to such information and limit further use and disclosures of such personal information to those purposes that make the return or destruction infeasible, for so long as Contractor, or any of its agents or subcontractors, maintains such information.

12. Due Diligence

Contractor shall exercise due diligence to ensure that it remains in compliance with this Agreement and is in compliance with the applicable provisions of HIPAA, HIPAA Regulations, the HITECH Act, and any more stringent applicable state law protecting PHI, and require its subcontractors and agents to be in compliance with the same.

13. Sanctions and/or Penalties

Contractor understands and acknowledges that it is required to comply with the provisions of HIPAA, HIPAA Regulations, the HITECH Act, and any more stringent applicable state law protecting PHI, and that failure to comply with these laws may

result in the imposition of civil and/or criminal sanctions and/or other penalties on Contractor as set forth under HIPAA, HIPAA Regulations and the HITECH Act.

14. Employee Training and Discipline

A. Contractor shall use reasonable measures to ensure compliance with the requirements of this Agreement. In doing so, Contractor must provide, at its own expense, annual security and privacy training on HIPAA to its employees who create, receive, maintain or transmit PHI or electronic PHI on behalf of DDS in accordance with 45 CFR § 164.308(a)(5)(i). Contractor shall require each employee who receives this training to sign a certification indicating the employee's name and the date on which the training was completed. Contractor shall retain each employee's written certifications for DDS inspection for a period of three years following contract termination.

B. Contractor also agrees to discipline employees who intentionally violate any provisions of this Agreement, including up to termination of employment.

15. Audits, Inspection and Enforcement

From time to time, DDS may inspect the facilities, systems, books and records of Contractor to monitor compliance with this Agreement. Contractor shall promptly remedy any violation of any provision of this Agreement and shall certify the same to the DDS Privacy Officer in writing. The fact that DDS inspects, or fails to inspect, or has the right to inspect, Contractor's facilities, systems and procedures does not relieve Contractor of its responsibility to comply with this Agreement, nor does DDS's:

A. Failure to detect; or
B. Detection, but failure to notify Contractor or require Contractor's remediation of any unsatisfactory practices, constitute acceptance of such practice or a waiver of DDS enforcement rights under this Agreement.

If Contractor 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 Agreement, Contractor shall notify DDS and provide DDS with a copy of any PHI or electronic PHI that Contractor provides to the Secretary or the Office of Civil Rights concurrently with providing such PHI or electronic PHI to the Secretary. Contractor is responsible for any civil or criminal penalties assessed due to an audit or investigation of Contractor in accordance with 42 USC § 17934(c).

16. Obligations of DDS

A. ***Notice of Privacy Practices.*** DDS shall provide Contractor with the Notice of

Privacy Practices that DDS produces in accordance with 45 CFR § 164.520, as well as any changes to such notice. Visit www.dds.ca.gov to view the most current Notice of Privacy Practices.

B. ***Permission by Individuals for Use and Disclosure of PHI.*** DDS shall provide Contractor, in writing, with any changes in, or revocation of, permission by an individual to use or disclose PHI or electronic PHI, if such changes affect the Contractor's permitted or required uses and disclosures.

C. ***Notification of Restrictions.*** DDS shall notify Contractor, in writing, of any restriction to the use or disclosure of PHI that DDS has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Contractor's use or disclosure of PHI.

D. ***Requests Conflicting with HIPAA Rules.*** DDS shall not request Contractor to use or disclose PHI or electronic PHI in any manner that would not be permissible under HIPAA, HIPAA Regulations, the HITECH Act, or any more stringent applicable state law protecting PHI.

17. Miscellaneous

A. ***Disclaimer***. DDS makes no warranty or representation that compliance by Contractor with this Agreement, HIPAA, HIPAA Regulations or the HITECH Act, will be adequate or satisfactory for Contractor's own purposes or any information in Contractor's possession or control, or transmitted or received by Contractor, is or will be secure from unauthorized access, viewing, use, or disclosure. Contractor is solely responsible for all decisions made by Contractor 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 Agreement 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, HIPAA Regulations, the HITECH Act, , and other applicable laws relating to the security or privacy of PHI and/or electronic PHI. Upon DDS's request Contractor agrees to promptly enter into good faith negotiations with DDS concerning an amendment to this Agreement embodying written assurances consistent with the standards and requirements of HIPAA, HIPAA Regulations, and the HITECH Act, or other applicable laws. If negotiations are unsuccessful, DDS may move to terminate this Agreement in the event:

1) Contractor does not promptly enter into negotiations to amend this Agreement when requested by DDS pursuant to this Section, or

2) Contractor does not enter into an amendment providing assurances regarding the safeguarding of PHI that DDS deems sufficient to satisfy the standards and requirements of HIPAA, HIPAA Regulations, and the HITECH Act.

C. ***Assistance in Litigation or Administrative Proceedings.*** Contractor shall make available to DDS, at no cost to DDS, its employees, subcontractors and/or agents to testify as witnesses, or otherwise, in the event litigation or administrative proceedings are commenced against DDS, its officers or employees, based upon a claimed violation of HIPAA, HIPAA Regulations, the HITECH Act or any more stringent applicable state law protecting PHI, which involve the inactions or actions by Contractor. This provision does not apply where Contractor or its subcontractor, employee or agent is a named adverse party to DDS.

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

E. ***Interpretation.*** The terms and conditions in this Agreement shall be interpreted as broadly as necessary to implement and comply with HIPAA, HIPAA Regulations, the HITECH Act, and any more stringent applicable state law protecting PHI. The parties agree that any ambiguity in the terms and conditions of this Agreement shall be resolved in favor of a meaning that complies and is consistent with HIPAA, HIPAA Regulations , the HITECH Act, , and any more stringent applicable state law protecting PHI.

F. ***References***. A reference in the terms and conditions of this Agreement to a section in HIPAA, HIPAA Regulations, and/or the HITECH Act means the section currently in effect or as amended.

G. ***Survival***. The respective rights and obligations of Contractor in this Agreement shall survive the termination or expiration of this 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.

References:

United States Department of Health and Human Services, Office for Civil Rights, Medical Privacy - National Standards to Protect the Privacy of Personal Health Information hhs.gov/ocr/hipaa

United States Department of Health and Human Services, Centers for Medicare and Medicaid Services – Security Standards www.cms.hhs.gov/SecurityStandard/

National Institute of Standards and Technology (NIST)
nist.gov/

FEDERAL INFORMATION PROCESSING STANDARDS (FIPS)

csrc.nist.gov/publications/PubsFIPS.html

Revision History:

Date	Description of Change	Reviewer
12/29/2017	Issue new Global version for use with non-state entities	Privacy Officer

EXHIBIT G, ATTACHMENT G-2

California Department of Corrections and Rehabilitation Cases

Involuntary medication of prisoners
(Pen. Code, § 2602 – formerly known as the *Keyhea* injunction) and

Appointment of a surrogate decision maker to make medical care decisions on behalf of an inmate patient who is not competent to make such decisions
(Pen. Code, § 2604)

BUSINESS ASSOCIATES AGREEMENT (HIPAA)
(undated)

FACILITATION OF PENAL CODE SECTIONS 2602 AND 2604 HEARINGS

WHEREAS, Provider, hereinafter referred to in this Exhibit as "Business Associate," acknowledges that the CDCR, hereinafter referred to in this Exhibit as "Covered Entity," has in its possession data that contains individual identifiable health information as defined by the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (HIPAA) and the regulations promulgated thereunder;

WHEREAS, Business Associate and Covered Entity acknowledge that the fulfillment of the Parties' obligations under this Service Agreement (Agreement) necessitates the exchange of, or access to, data including individual identifiable health information; and,

WHEREAS, the parties desire to comply with federal and California laws regarding the use and disclosure of individually identifiable health information, and in particular with the provisions of HIPAA and the regulations promulgated thereunder.

NOW, THEREFORE, in consideration of the mutual promises and covenants hereinafter contained, the Parties agree as follows:

ARTICLE 1 DEFINITIONS

The following terms and others used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use. Terms used, but not otherwise defined, in this Exhibit shall have the meanings set forth below.

1.1 “Business Associate” shall generally have the same meaning as the term “business associate” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean the contractor to the contract to which this Business Associate Agreement is attached as an exhibit. For purposes of this exhibit only, the term “Agreement” shall refer to this Business Associate Agreement. The term “Service Agreement” shall refer to the contract to which this Business Associate Agreement is attached as an exhibit.

1.2 “Covered Entity” shall general have the same meaning as the term “covered entity” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean California Department of Corrections and Rehabilitation, California Correctional Healthcare Services (CCHCS).

1.3 “HIPAA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

1.4 "HHS Transaction Standard Regulation" means the Code of Federal Regulations (CFR) at Title 45, part 160 and 162.

1.5 “Individual” means the subject of protected health information (PHI) or, if deceased, his or her personal representative.

1.6 "Parties" shall mean the Covered Entity and Business Associate. (Covered Entity and Business Associate, individually, may be referred to as a Party.)

1.7 “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.

1.8 “PHI” shall have the same meaning as the term “protected health information” in 45 CFR part 164.501, limited to the information created or received by Business Associate from or on behalf of the Covered Entity.

1.9 “Required By Law” shall have the same meaning as “required by law” in 45 CFR part 164.501.

2.0 “Secretary” shall mean the Secretary of the Department of Health and Human Services or his designee.

Any other terms used, but not otherwise defined, in this Exhibit shall have the same meaning as those terms in the Privacy Rule.

ARTICLE 2 CONFIDENTIALITY

2.1 Obligations and Activities of Business Associate. Business Associate agrees as follows:

(a) not to use or further disclose PHI other than as permitted or required by this Agreement or as required by law;

(b) to establish, maintain, and use appropriate safeguards to prevent use or disclosure of the PHI other than as permitted herein;

(c) to report to Covered Entity any use, access, or disclosure of the PHI not provided for by this Agreement, or any misuse of the PHI, including but not limited to systems compromises of which it becomes aware and to mitigate, to the extent practicable, any harmful effect that is known to Business Associate as a result thereof. Business Associate shall be responsible for any and all costs (including the costs of Covered Entity) associated with mitigating or remedying any violation of this Agreement;

(d) to enforce and maintain appropriate policies, procedures, and access control mechanisms to ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created, or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information. The access and privileges granted to any such agent shall be the minimum necessary to perform the assigned functions;

(e) to provide access, at the request of Covered Entity, and in the time and manner reasonable designated by Covered Entity, to PHI in a Designated Record Set (as defined in the Privacy Rule), to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR part 164.524;

(f) to make any amendment(s) to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR part 164.526 at the request of Covered Entity or an Individual, and in the time and manner reasonably requested by Covered Entity.

(g) to make internal practices, books, and records relating to the use and disclosure of PHI received from, or created, or received by Business Associate on behalf of, Covered Entity available to the Covered Entity, or at the request of the Covered Entity to the Secretary, in a time and manner reasonably requested by Covered Entity or designated by the Secretary, for purposes of the Secretary determining Covered Entity’s compliance with the Privacy Rule.

(h) to document such disclosures of PHI, and information related to such disclosures, as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR part 164.528. Said documentation shall include, but not be limited to, the date of the disclosure, the name and, if known, the address of the recipient of the PHI, a brief description of the PHI disclosed, and the purpose of the disclosure. Said documentation shall be made available to Covered Entity upon request.

(i) to provide to Covered Entity or an Individual, in a time and manner reasonably requested by Covered Entity, information collected in accordance with section 2.1(h) above to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR part 164.528.

(j) to promptly notify Covered Entity of all actual or suspected instances of deliberate unauthorized attempts (both successful and unsuccessful) to access PHI. Such notice shall be made to Covered Entity by telephone as soon as Business Associate becomes aware of the unauthorized attempt, and this telephone notification shall be followed within two (2) calendar days of the discovery of the unauthorized attempt by a written report to Covered Entity from Business Associate. Business Associate shall, at the same time, report to Covered Entity any remedial action taken, or proposed to be taken, with respect to such unauthorized attempt. Covered Entity shall have the discretion to determine whether or not any such remedial action is sufficient, and all such remedial action shall be at Business Associate's expense.

(k) to maintain and enforce policies, procedures, and processes to protect physical access to hardware, software, and/or media containing PHI (e.g., hardcopy, tapes, removable media, etc.) against unauthorized physical access during use, storage, transportation, disposition and /or destruction.

(l) to ensure that access controls in place to protect PHI and processing resources from unauthorized access are controlled by two-factor identification and authentication: a user ID and a Token, Password, or Biometrics.

(m) to implement, use and monitor its compliance with appropriate technological, administrative, and physical safeguards to prevent the use or disclosure of PHI other than as permitted by this Agreement. Business Associate shall provide Covered Entity with evidence of such safeguards upon Covered Entities request.

Covered Entity has the right to determine, in its sole discretion, whether such safeguards are appropriate, and to require any additional safeguards it deems necessary.

(n) In the event that Business Associate is served with legal process (e.g., a subpoena) or request from a governmental agency (e.g., the Secretary) that potentially could require the disclosure of PHI, Business Associate shall provide prompt (i.e., within twenty-four (24) hours) written notice of such legal process (including a copy of the legal process served) to the designated person at the Covered Entity. In addition, Business Associate shall not disclose the PHI without the consent of Covered Entity unless pursuant to a valid and specific court order or to comply with a requirement for review of documents by a governmental regulatory agency under its statutory or regulatory authority to regulate the activities of either party.

(o) to submit to periodic audits by Covered Entity verifying Business Associate's compliance with appropriate technological, administrative, and physical safeguards to prevent the use or disclosure of PHI other than as permitted by this Agreement, as well as compliance with the terms and conditions pursuant to this Agreement and compliance with state and federal laws and regulations. Audit review may be undertaken directly by the Covered Entity or by third parties engaged by the Covered Entity. Business Associate shall cooperate fully with Covered Entity or any such third party in connection with such audits.

2.2 Disclosures Required By Law.

In the event that Business Associate is required by law to disclose PHI, Business Associate will immediately provide Covered Entity with written notice and provide Covered Entity an opportunity to oppose any request for such PHI or to take whatever action Covered Entity deems appropriate.

2.3 Specific Use and Disclosure Provisions.

(a) Except as otherwise limited in this Agreement, Business Associate may use PHI only to carry out the legal responsibilities of the Business Associate under this Agreement.

(b) Except as otherwise limited in this Agreement, Business Associate may only disclose PHI (i) as Required By Law, or (ii) in the fulfillment of its obligations under the Agreement and provided that Business Associate has first obtained (A) the consent of Covered Entity for such disclosure, (B) reasonable assurances from the person to whom the information is disclosed that the PHI will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and (C) reasonable assurances from the person to whom the information is disclosed that such person will notify the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

2.4 Obligations of Covered Entity.

(a) Covered Entity shall notify Business Associate of any limitations in its notice of privacy practices of Covered Entity in accordance with 45 CFR part164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

(b) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosures of PHI.

(c) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR part 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

(d) For any PHI received by Covered Entity from Business Associate on behalf of a third party or another covered entity, Covered Entity agrees to be bound to the obligations and activities of Business Associate enumerated in section 2.1 as if and to the same extent Covered Entity was the named Business Associate hereunder.

2.5 Permissible Requests by Covered Entity.

Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by the Covered Entity.

2.6 Policy and Procedure Review.

Upon request, Business Associate shall make available to Covered Entity any and all documentation relevant to the safeguarding of PHI including but not limited to current policies and procedures, operational manuals and/or instructions, and/or employment and/or third party agreements.

ARTICLE 3 SECURITY

3.1 Government Healthcare Program Representations.

Business Associate hereby represents and warrants to Covered Entity, its shareholders, members, directors, officers, agents, or employees have not been excluded or served a notice of exclusion or have been served with a notice of proposed exclusion, or have

committed any acts which are cause for exclusion, from participation in, or had any sanctions, or civil or criminal penalties imposed under, any federal or state healthcare program, including but not limited to Medicare or Medicaid, or have been convicted, under federal or state law (including without limitation a plea of nolo contendere or participation in a first offender deterred adjudication or other arrangement whereby a judgment of conviction has been withheld), of a criminal offense related to (a) the neglect or abuse of a patient, (b) the delivery of an item or service, including the performance of management or administrative services related to the delivery of an item or service, under a federal or state healthcare program, (c) fraud, theft, embezzlement, breach of fiduciary responsibility, or other financial misconduct in connection with the delivery of a healthcare item or service or with respect to any act or omission in any program operated by or financed in whole or in party by any federal, state or local government agency, (d) the unlawful, manufacture, distribution, prescription, or dispensing of a controlled substance, or (e) interference with or obstruction of any investigation into any criminal offense described in (a) through (d) above. Business Associate further agrees to notify Covered Entity immediately after Business Associate becomes aware that the foregoing representation and warranty may be inaccurate or may be incorrect.

3.2 Security Procedures.

Each Party shall employ security procedures that comply with HIPAA and all other applicable state and federal laws and regulations (collectively, the Law) and that are commercially reasonable, to ensure that transactions, notices, and other information that are electronically created, communicated, processed, stored, retained or retrieved are authentic, accurate, reliable, complete, and confidential. Moreover, each Party shall, and shall require any agent or subcontractor involved in the electronic exchange of data to:

(a) require its agents and subcontractors to provide security for all data that is electronically exchanged between Covered Entity and Business Associate;

(b) provide, utilize, and maintain equipment, software, services, and testing necessary to assure the secure and reliable transmission and receipt of data containing PHI;

(c) maintain and enforce security management policies and procedures and utilize mechanisms and processes to prevent, detect, record, analyze, contain, and resolve unauthorized access attempts to PHI or processing resources;

(d) maintain and enforce policies and guidelines for workstation use that delineate appropriate use of workstations to maximize the security of data containing PHI;

(e) maintain and enforce policies, procedures, and a formal program for periodically reviewing its processing infrastructure for potential security vulnerabilities;

(f) implement and maintain, and require its agents and subcontractors to implement and maintain, appropriate and effective administrative, technical, and physical safeguards to protect the security, integrity, and confidentiality of data

electronically exchanged between Business Associate and Covered Entity, including access to data as provided herein. Each Party and its agents and subcontractors shall keep all security measures current and shall document its security measures implemented in written policies, procedures or guidelines, which it will provide to the other Party upon their request.

ARTICLE 4
EXCHANGE OF STANDARD TRANSMISSIONS

4.1 Obligations of the Parties. Each of the Parties agrees that for the PHI,

(a) it will not change any definition, data condition, or use of a data element or segment as proscribed in the HHS Transaction Standard Regulation.

(b) it will not add any data elements or segments to the maximum denied data set as proscribed in the HHS Transaction Standard Regulation.

(c) it will not use any code or data elements that are either marked "not used" in the HHS Standard's implementation specifications or are not in the HHS Transaction Standard's implementation specifications.

(d) it will not change the meaning or intent of any of the HHS Transaction Standard's implementation specifications.

4.2 Incorporation of Modifications to HHS Transaction Standards.

Each of the Parties agrees and understands that from time-to-time, HHS may modify and set compliance dates for the HHS Transaction Standards. Each of the Parties agrees to incorporate by reference into this Agreement any such modifications or changes.

1.3 Code Set Retention.

If applicable, both Parties understand and agree to keep open code sets being processed or used in this Agreement for at least the current billing period or any appeal period, whichever is longer.

1.4 Business Associate Obligations.

(a) Business Associate assumes all liability for any damage, whether direct or indirect, stemming from Business Associate's non-compliance with HHS Transaction Standards with regards to its handling of Covered Entity's electronic data.

(b) Business Associate assumes all liability from any claim, loss or damage of any kind, whether direct or indirect, whether to person or property, arising out of or related to Business Associate's use or unauthorized disclosure of the Covered Entity's electronic data.

(c) Business Associate agrees to maintain adequate back-up files to recreate transmissions in the event that such recreations become necessary. Back-up files shall be subject to this Agreement to the same extent as original data.

(d) Business Associate agrees to trace lost or indecipherable transmissions and make reasonable efforts to locate and translate the same. Business Associate shall bear all costs associated with the recreation of incomplete, lost, or indecipherable transmissions if such loss is the result of an act or omission of Business Associate.

(e) Business Associate shall maintain electronic copies of any of Covered Entity's data that may be lodged or filed with Business Associate, in accordance with Business Associate's record retention policy..

(f) Except encounter data furnished by Business Associate to Covered Entity, Business Associate shall not (other than to correct errors) modify any data to which it is granted access under this Agreement or derive new data from such existing data. Any modification of data is to be recorded, and a record of such modification is to be retained by Business Associate for a period of seven (7) years.

(g) Business Associate shall not disclose security access codes to any third party in any manner without the express written consent of Covered Entity. Business Associate furthermore acknowledges that Covered Entity may change such codes at any time without notice. Business Associate shall assume responsibility for any damages arising from its disclosure of the security access codes or its failure to prevent any third party use of the system without the express written consent of Covered Entity.

ARTICLE 5 MISCELLANEOUS

5.1 Term and Termination.

(a) Term. The Term of this Agreement shall be effective as of the first date of commencement of services under this entire Agreement, and shall terminate when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in this section.

(b) Termination for Cause. Upon a material breach by Business Associate of its obligation hereunder, Covered Entity may (i) terminate this Agreement and the Service Agreement; (ii) permit Business Associate to cure the breach; (iii) report the violation to the Secretary; and/or (iv) require Business Associate to take such other action as Covered Entity may request, at Business Associate's expense.

Covered Entity's remedies under this paragraph shall be cumulative, and the exercise of any remedy shall not preclude the exercise of any other. If Covered Entity elects to terminate the Agreement pursuant to a breach of terms and conditions of this Exhibit, Covered Entity shall be relieved of any further obligations under the entire Agreement, and shall be immediately entitled to a refund of any amounts prepaid from the date of the termination through the end of the payment period, on a pro rata basis.

The foregoing termination language is in addition to any other termination language set forth in the entire Agreement.

(c)Effect of Termination.

(i)Except as provided in paragraph 5.1(c)(ii), upon termination of this Agreement, for any reason, Business Associate shall maintain the integrity of such PHI in accordance with Business Associate's record retention schedule.

5.3 Disputes.

HIPAA Appeal Procedures

CDCR has established and shall maintain an appeal procedure in accordance with CDCR Department Operations Manual, section 22040.16. Business Associate agrees that disputes arising under the terms of this Exhibit shall be resolved in accordance with the following:

1. Verbal Appeal

Business Associate and CDCR's Privacy Officer shall first attempt to resolve the problem by informal discussion. Business Associate agrees that CDCR's Division of Correctional Health Care Services shall be used as a resource in solving potential disputes.

2. Informal Appeal

If the issue is not resolved at the verbal appeal level, Business Associate shall file, within thirty (30) working days, an informal written appeal specifying: the issue(s) of dispute, legal authority or other basis for Business Associate's position, supporting evidence, and remedy sought, with the CDCR Chief, Licensing and Information Systems, and provide a photocopy to the CDCR Assistant Deputy Director, Office of Business Services. The CDCR Chief, Licensing and Information Systems, shall make a determination on the issue and respond in writing within thirty (30) working days of receipt of the informal appeal, indicating the decision reached.

3. Formal Appeal

Should Business Associate disagree with the informal appeal decision, Business Associate shall submit, within ten (10) working days after Business Associate's receipt of the decision of the informal appeal, to the CDCR Deputy Director, Division of Correctional Health Care Services, and a photo copy to the CDCR, Assistant Deputy Director, Office of Business Services, written notification indicating why the informal appeal decision is unacceptable, along with a copy of the original statement of dispute and a copy of CDCR's response. The CDCR Deputy Director, Division of Correctional Health Care Services, or his/her designee may meet with Business Associate to review the issues within twenty (20) working days of the receipt of Business Associate's notification and shall provide Business Associate with written notification of the decision within forty-five (45) working days from the receipt of the formal appeal.

The foregoing dispute process is solely for the purpose of disputes arising from the terms and conditions of this Exhibit. Disputes in relation to the scope of work and other terms and conditions shall be in accordance with any other dispute language set forth in the entire Agreement.

5.4 Injunctive Relief.

Notwithstanding any rights or remedies provided for in section 5.3, Covered Entity retains all rights to seek injunctive relief to prevent the unauthorized use of disclosure of PHI by Business Associate or any agent, contractor or third party that received PHI from Business Associate.

5.5 Regulatory References.

A reference in this Agreement to a part in the Privacy Rule means the part as in effect or as amended.

5.6 Amendment.

The Parties agree to take such action as is necessary to amend this Agreement from time to time to the extent necessary for Covered Entity to comply with the requirements of HIPAA and its regulations. All amendments to this Exhibit shall be in writing and signed by both Parties through a formal amendment to the entire agreement.

5.7 Survival.

The respective rights and obligations of Business Associate and Covered Entity under sections 4.5, 5.1 and 5.2(c) of this Agreement shall survive the termination of this Agreement.

5.8 Limitation of Damages.

Other than liabilities under section 5.1, neither Party shall be liable to the other for any special, incidental, exemplary, punitive, or consequential damages arising from or as a result of any delay, omission, or error in the electronic transmission or receipt of any information pursuant to this Agreement, even if the other Party has been advised of the possibility of such damages.

5.9 Interpretation.

Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

5.10 Third Party Beneficiary

Unless otherwise set forth herein, nothing contained herein is intended, nor shall it be construed, to create rights running of the benefit of third parties.

5.11 Notices

Any HIPAA related notice required hereunder shall be deemed to be sufficient if mailed to the parties at the addresses below. In order to avoid unreasonable delay in the provision of the services to be rendered pursuant to this Agreement, Business Associate and Covered Entity shall each designate a specific HIPAA representative(s) for the purpose of communication between the Parties. Such representative(s) may be changed upon written notice to the other party.

Business Associate:

Bob Varma

Deputy Director and Assistant Chief Administrative Law Judge Office of Administrative Hearings

2349 Gateway Oaks Drive, Suite 200

Sacramento, CA 95833

Telephone: **REDACTED**

Covered Entity:

California Department of Corrections and Rehabilitation Privacy Officer

HIPAA Compliance Unit

California Correctional Health Care Services

P.O. 588500, Suite C-3

Elk Grove, CA 95758 Telephone: **REDACTED**

THE REST OF THIS PAGE IS BLANK

EXHIBIT G, ATTACHMENT G-3

California Department of Corrections and Rehabilitation
California Correctional Health Care Services
Professional Practices Executive Committee Cases

Privileges of a licensed practitioner
(Bus. & Prof. Code, § 809 et seq.)

HIPAA BUSINESS ASSOCIATE AGREEMENT and
INFORMATION SECURITY AGREEMENT

HIPAA BUSINESS ASSOCIATE AGREEMENT
Recitals – STANDARD RISK
(New CCHCS version 6/21/2021)

A. This Contract (Agreement) constitutes a business associate relationship under the Health Insurance Portability and Accountability Act (HIPAA) and its implementing privacy and security regulations at 45 C.F.R. Parts 160 and 164 (collectively, the HIPAA regulations).

B. The California Department of Corrections and Rehabilitation, California Correctional Health Care Services (CCHCS) wishes to disclose to Business Associate certain information pursuant to the terms of this Agreement, some of which may constitute Protected Health Information (PHI) and confidential information protected by Federal and/or state laws.

C. Protected Health Information or PHI means any information, whether oral or recorded in any form or medium that relates to the past, present, or future physical or mental condition of an individual, the provision of health and dental care to an individual, or the past, present, or future payment for the provision of health and dental care to an individual; and that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. PHI shall have the meaning given to such term under HIPAA and HIPAA regulations, as the same may be amended from time to time. Confidential Information means information protected by Federal and/or state laws identified in this Agreement.

D. Unsecured Protected Health Information means protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified in guidance from the Secretary of the U.S. Department of Health and Human Services (Secretary).

E. Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI, or confidential information 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.

F. As set forth in this Agreement, the Contractor is the Business Associate of CCHCS that provides services, medical items for identified patients, arranges, performs or assists in the performance of functions or activities on behalf of CCHCS and creates, receives, maintains, transmits, uses or discloses PHI.

G. CCHCS and Business Associate desire to protect the privacy and provide for the security of PHI and confidential information created, received, maintained, transmitted, used or disclosed pursuant to this Agreement, in compliance with HIPAA, HIPAA regulations, and other applicable laws.

H. The purpose of the Business Associate Agreement (BAA) is to satisfy certain standards and requirements of HIPAA and the HIPAA regulations.

I. The terms used in this Agreement, but not otherwise defined, shall have the same meanings as those terms in the HIPAA regulations.

In exchanging information pursuant to this Agreement, the parties agree as follows:

1. Permitted Uses and Disclosures of PHI by Business Associate

A. ***Permitted Uses and Disclosures***. Except as otherwise indicated in this Agreement, Business Associate may use or disclose PHI only to perform functions, activities or services specified in this Agreement, for, or on behalf of CCHCS, provided that such use or disclosure would not violate the HIPAA regulations, if done by CCHCS.

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

1) ***Use and disclose for management and administration***. Use and disclose PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided that 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.

2) ***Provision of Data Aggregation Services.*** Use PHI to provide data aggregation services to CCHCS. Data aggregation means the combining of PHI created or received by the Business Associate on behalf of CCHCS 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 CCHCS.

2. Responsibilities of Business Associate

Business Associate agrees:

A. ***Nondisclosure.*** Not to use or disclose PHI other than as permitted or required by this Agreement or as required by law.

B. ***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 CCHCS; and to prevent use or disclosure of PHI other than as provided for by this Agreement. 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 C, Security, below. Business Associate will provide CCHCS with an attestation that its current and regularly updated internal privacy and information security policies comply with this requirement. CCHCS retains the right to inspect Business Associate's information privacy and security program if Business Associate does not provide an attestation.

C. ***Security***. To take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI, and provide data security procedures for the use of CCHCS at the end of the contract period. These steps shall include, at a minimum:

1) Complying with all of the data system security precautions listed in this Agreement or in an Exhibit incorporated into this Agreement; and

2) Complying with the safeguard provisions in the Department's Information Security Policy, embodied in the Security and Risk Management Policy in the Information Technology Section of the State Administrative Manual (SAM), § 4840 et seq., Information Security Policy in SAM § 5300, et. seq. and State Information Management Manual (SIMM) § 5300 et. seq. in so far as the security standards in these manuals apply to Business Associate's operations. 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 safeguards that provide 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 this Agreement.

Business Associate shall designate an Information 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 CCHCS.

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

E. ***Business Associate's Agents***. To ensure that any agents, including subcontractors, to whom Business Associate provides PHI received from or created or received by Business Associate on behalf of CCHCS, agree to the same restrictions and conditions that apply to Business Associate with respect to such PHI, including implementation of reasonable and appropriate administrative, physical, and technical safeguards to protect such PHI; and to incorporate, when applicable, the relevant provisions of this Agreement into each subcontract or with agents or subcontractors.

F. ***Availability of Information to* CCHCS *and Individuals***. To provide access as CCHCS may require, and in the time and manner designated by CCHCS (upon reasonable notice and during Business Associate's normal business hours) to PHI in a Designated Record Set, to CCHCS (or, as directed by CCHCS), to an Individual, in accordance with 45 C.F.R. § 164.524. Designated Record Set means the group of records maintained for CCHCS that includes medical, dental and billing records about individuals; enrollment, payment, claims adjudication, and case or medical management systems maintained for CCHCS health plans; or those records used to make decisions about individuals on behalf of CCHCS. Business Associate shall use the forms and processes developed by CCHCS for this purpose and shall respond to requests for access to records transmitted by CCHCS within fifteen (15) calendar days of receipt of the request by producing the records or verifying that there are none.

G. ***Amendment of PHI***. To make any amendment(s) to PHI that CCHCS directs or agrees to pursuant to 45 C.F.R. § 164.526, in the time and manner designated by CCHCS.

H. ***Internal Practices***. To make Business Associate's internal practices, books and records relating to the use and disclosure of PHI received from CCHCS, or created or received by Business Associate on behalf of CCHCS, available to CCHCS or to the Secretary in a time and manner designated by CCHCS or by the Secretary, for purposes of determining CCHCS compliance with the HIPAA regulations.

I. ***Documentation of Disclosures***. To document and make available to CCHCS (within 14 calendar days) or (at the direction of CCHCS) 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 45 C.F.R. § 164.528.

J. ***Notification of Patient Confidential Communications.*** Notify CCHCS (within 2 calendar days of request) of any patient (or patient's representative) preferences (or changes to) regarding method of or how to communicate with the patient.

K. ***Notification of Information Security Incidents, Investigation, and Written Reporting***.

1) ***Discovery of Information Security Incident***. To notify CCHCS ***immediately by telephone call plus email/electronic communication*** upon the discovery of an information security incident involving the privacy of or security of PHI in computerized form if the PHI was, or is reasonably believed to have been, acquired by an unauthorized person, or ***within 24 hours by email/electronic communication*** of any suspected security incident, intrusion or unauthorized use or disclosure of PHI in violation of this Agreement, or potential loss of confidential data affecting this Agreement. Notification shall be provided to the CCHCS contract manager, the CCHCS Privacy Officer, and the CCHCS Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves electronic PHI, notification shall be provided by calling the CCHCS ITSD Solution Center at **1-888-735-3470**. Business Associate shall take:

   i. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment, including potential claims or exemptions or exceptions following mitigation; and
   ii. Any and all actions pertaining to such unauthorized disclosures required by applicable Federal and State laws and regulations.

2) ***Investigation of Information Security Incident and Status Reporting to CCHCS***. To immediately investigate such information security incident, breach, or unauthorized use or disclosure of PHI. Within 72 hours of the discovery, to notify and provide the status of the investigation to the CCHCS contract manager(s), the CCHCS Privacy Officer, and the CCHCS Information Security Officer of:

   i. What data elements were involved and the extent of the data involved in the breach,
   ii. A description of the unauthorized persons known or reasonably believed to have improperly used, disclosed, or received PHI,
   iii. A description of where the PHI is believed to have been improperly transmitted, sent, orutilized,
   iv. A description of the probable causes of the improper use or disclosure; and
   v. Whether Civil Code § 1798.29 or § 1798.82 or any other federal or state laws requiring individual notifications of breaches are triggered.

3) ***Written Report***. To provide an initial written report of the investigation to the CCHCS contract managers, the CCHCS Privacy Officer, and the CCHCS Information Security Officer within ten (10) calendar days of the information security incident, discovery of the breach, or discovery of unauthorized use, disclosure, or receipt. The report shall be in the form and manner required by CCHCS and includes, but is not limited to, the information specified above, as well as a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. The initial report shall be submitted using the CCHCS Information Security Incident Reporting Form (ISIR) attached hereto as Attachment 1 to this Agreement. The ISIR shall be emailed to the CCHCS Information Security Office at **REDACTED**. Business Associate shall provide supplemental reports, as necessary, as the investigation progresses, and at the request of CCHCS. CCHCS retains all rights as the Covered Entity to review the sufficiency of

the BA's notice, investigation, or reporting of information security incidents involving its PHI.

4) ***Notification of Individuals***. To notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal law and to pay any costs of such notifications, as well as any costs associated with the breach. The CCHCS contract managers, the CCHCS Privacy Officer, and the CCHCS Information Security Officer shall approve the time, manner and content of any such notifications prior to release of the notification.

5) CCHCS ***Contact Information***. To direct communications to the above referenced CCHCS staff, the Contractor shall initiate contact as indicated herein CCHCS 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 Agreement.

CCHCS	**CCHCS**	**CCHCS**
Contract Manager	**Privacy Officer**	**Information Security Officer**
See Exhibit A for Contract Manager information See the Scope of Work exhibit for Program Contract Manager Information	Privacy Officer California Correctional Health Care Services P.O. Box 588500, Bldg. D3, Elk Grove, CA 95758 Email: **REDACTED** Telephone: **REDACTED**	Information Security Officer Information Security Officer CCHCS Information Technology Services Division P.O. Box 588500, Bldg. C3, Elk Grove, CA 95758 Email: **REDACTED** Telephone: **REDACTED**

L. ***Employee Training and Discipline***. To train and use reasonable measures to ensure compliance with the requirements of this Agreement by employees who assist in the performance of functions or activities on behalf of CCHCS under this Agreement and use or disclose PHI; and discipline such employees who intentionally violate any provisions of this Agreement, including by termination of employment. In complying with the provisions of this section L, Business Associate shall observe the following requirements:

1) Business Associate shall provide information privacy and security training, at least every twelve (12) calendar months, at its own expense, to all its employees who assist in the performance of functions or activities on behalf of CCHCS under this Agreement and use or disclose PHI.

2) Business Associate shall require each employee who receives information privacy and security training to sign a certification, indicating the employee's name and the date on which the training was completed.

3) Business Associate shall retain each employee's written certifications for CCHCS inspection for a period of three years following contract termination, and shall provde copies of training certifications to CCHCS on request.

3. Obligations of CCHCS

CCHCS agrees to:

A. ***Notice of Privacy Practices***. Provide Business Associate with the Notice of Privacy Practices that CCHCS produces in accordance with 45 C.F.R. § 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 CCHCS has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect the Business Associate's use or disclosure of PHI.

D. ***Notification of Patient Confidential Communications.*** Notify the Business Associate (within 2 calendar days of request) of any patient (or patient's representative) preferences (or changes to) regarding the method of or how to communicate with the patient.

E. ***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.

4. Audits, Inspection and Enforcement

From time to time, CCHCS may inspect the facilities, systems, books and records of Business Associate to monitor compliance with this Agreement. Business Associate shall promptly remedy any violation of any provision of this Agreement and shall certify the same to the CCHCS Privacy Officer in writing. The fact that CCHCS inspects, or fails to inspect, or has the right to inspect, Business Associate's facilities, systems and procedures does not relieve Business Associate of its responsibility to comply with this Agreement, nor does CCHCS':

A. Failure to detect; or

B. 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 CCHCS enforcement rights under this Agreement and this Agreement.

Business Associate may meet this requirement by providing a SOC2 certificate of compliance or other certificate of compliance to nationally recognized information security standards and procedures by an accreditation body acceptable to CCHCS. Business

Associate shall ensure SOC2 or other compliance certificates are valid and in effect for the duration of any contract to which this BAA attaches.

5. Termination

A. ***Termination for Cause***. Upon CCHCS knowledge of a material breach of this Agreement by Business Associate, CCHCS shall:

1) Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement if Business Associate does not cure the breach or end the violation within the time specified by CCHCS;

2) Immediately terminate this Agreement if Business Associate has breached a material term and cure is not possible; or

3) If neither cure nor termination is feasible, report the violation to the Secretary.

B. ***Judicial or Administrative Proceedings***. Business Associate will notify CCHCS if it is named as a defendant in a criminal proceeding for a violation of HIPAA. CCHCS may terminate this Agreement if Business Associate is found guilty of a criminal violation of HIPAA. CCHCS may terminate this 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.

C. ***Effect of Termination***. Upon termination or expiration of this Agreement for any reason, Business Associate shall return or destroy all PHI received from CCHCS (or created or received by Business Associate on behalf of CCHCS that Business Associate still maintains in any form, and shall retain no copies of such PHI or, if return or destruction is not feasible, shall continue to extend the protections of this Agreement to such information, 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.

6. Miscellaneous Provisions

A. ***Disclaimer***. CCHCS makes no warranty or representation that compliance by Business Associate with this Agreement, 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 Agreement may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as necessary to implement the standards and requirements of HIPAA, the HIPAA regulations and other applicable laws relating to the security or privacy of PHI. Upon CCHCS request, Business Associate agrees to promptly enter into negotiations with CCHCS concerning an amendment to this Agreement confirming written assurances consistent with the standards and requirements of HIPAA, the HIPAA regulations or other applicable laws. CCHCS may terminate this Agreement upon thirty (30) days written notice in the event:

1) Business Associate does not promptly enter into negotiations to amend this Agreement when requested by CCHCS pursuant to this Section, or

2) Business Associate does not enter into an amendment providing assurances regarding the safeguarding of PHI that CCHCS in its sole discretion, deems 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 this Agreement, available to CCHCS at no cost to CCHCS to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CCHCS, 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 Agreement is intended to confer, nor shall anything herein confer, upon any person other than CCHCS or Business Associate and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

E. ***Interpretation.*** The terms and conditions in this Agreement shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HIPAA regulations and applicable state laws. The parties agree that any ambiguity in the terms and conditions of this Agreement shall be resolved in favor of a meaning that complies and is consistent with HIPAA and the HIPAA regulations.

F. ***Regulatory References***. A reference in the terms and conditions of this Agreement to a section in the HIPAA regulations means the section in effect or as amended during the Agreement term.

G. ***Survival***. The respective rights and obligations of Business Associate under Section 6.C of this Agreement shall survive the termination or expiration of this 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.

INFORMATION SECURITY AGREEMENT (ISA)
(Revision date January 15, 2016, Ver. 2.0)

1. Introduction and Purpose

a. This Information Security Agreement (ISA) outlines the Service Provider requirements for the collection, maintenance, and dissemination of any information that identifies or describes an individual in conjunction with the performance of services provided to CCHCS under any contract, purchase document, Memorandum of Understanding, or any other transaction involving information receipt or information exchange between CCHCS and the Service Provider.

b. This ISA does not substitute for any other addendum, attachment, exhibit or obligation with respect to protected health information and the applicability of and requirement to comply with the Health Information Portability and Accountability Act of 1996 (HIPAA) P.L. No. 104-191, 110 Stat. 1938 (1996), including the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

2. Definitions

a. The term “personal information” means any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual under the provisions of the California Information Practices Act (Civil Code Section 1798 et Seq.).

b. The term “public information” means information maintained by state agencies that is not exempt from disclosure under the provisions of the California Public Records Act (Government Code Sections 6250-6265) or other applicable state or federal laws.

c. The term “confidential information” means information maintained by state agencies that is exempt from disclosure under the provisions of the California Public Records Act (Government Code Sections 6250-6265) or has restrictions on disclosure in accordance with other applicable state or federal laws.

d. The term “sensitive information” means any public information or confidential information that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion as identified in Information Security Program Management Standard 5305-A of the California Statewide Information Management Manual (SIMM).

e. The term “service provider” means any vendor, contractor, subcontractor, or third party, including employees, independent contractors or consultants providing any service to CCHCS under this ISA.

3. Acknowledgments

a. As an entity engaged in a contract, agreement, memorandum of understanding (MOU) and/or information receipt and/or information exchange with CCHCS, you (herein referred to as the Service Provider) acknowledge and agree that in the course of contract, agreement, MOU by and as indicated beyond, Service Provider shall comply with applicable United States and California laws and regulations, including but not limited to Sections 14100.2 and 5328 et seq. of the Welfare and Institutions Code, Section 431.300 et seq. of Title 42, Code of Federal Regulations, the Health Insurance Portability and Accountability Act (HIPAA), including but not limited to Section 1320 d et seq., of Title 42, United States Code and its implementing regulations (including but not limited to Title 45, CFR, Parts 160, 162 and 164) regarding the confidentiality and security of individually identifiable health information (IIHI), California Medical Information Act, Lantermann-Petris-Short Act, Alcohol Substance and Abuse Act, California Public Records Act, California Information Practices Act of 1977, the California State Administrative Manual and its associated regulations, mandates, budget letters and memorandums, and the State Information Management Manual.

4. Standard of Care

a. Service Provider acknowledges and agrees that, in the course of its engagement by CCHCS, Service Provider may receive or have access to sensitive and/or private information.

b. Service Provider shall comply with the terms and conditions set forth in this ISA regarding creation, collection, receipt, management, sharing, exchanging, transmission, storage, disposal, use and disclosure of sensitive and confidential information.

c. Service Provider shall be responsible for, and remain liable to, CCHCS for the actions of unauthorized employees, contractors and subcontractors concerning the treatment of CCHCS related sensitive and confidential information, as if they were Service Provider’s own actions.

d. In recognition of the foregoing, Service Provider acknowledges and agrees it shall:

i. Treat sensitive and confidential information with such degree of care required by federal and state requirements including but not limited to the United States National Institute for Standards and Technology and the State Administrative Manual Chapter 5300.

ii. Collect, use and disclose sensitive and confidential information solely and exclusively for the purposes for which the information, or access to it, is provided pursuant to the terms and conditions of this ISA;

iii. Not use, sell, rent, transfer, distribute, or otherwise disclose or make available sensitive or confidential information for the benefit of anyone other than CCHCS without CCHCS's prior written consent.

5. Responsibilities of the Service Provider

a. The Service Provider is obligated to ensure the following:

i. Safeguards. To prevent the unauthorized creation, use, management, transfer, distribution, storage, etc. other than as provided for by this ISA. The Service Provider shall develop and maintain an information privacy and security program that includes the implementation of administrative, technical, and physical safeguards appropriate to the size and complexity of the Service Provider's operations and the nature and scope of its activities. The information privacy and security programs must reasonably and appropriately protect the confidentiality, integrity, and availability of the CCHCS information it creates, receives, maintains, or transmits; and prevent the use or disclosure of CCHCS information other than as provided for by this ISA. The Service Provider shall provide CCHCS with information concerning such safeguards as CCHCS may reasonably request from time to time.

ii. The Service Provider shall restrict logical and physical access to CCHCS sensitive and confidential information to authorized users only.

iii. The Service Provider shall implement appropriate authentication methods to ensure information system access to sensitive and confidential information. If passwords are used in user authentication (e.g., username/password combination), the Service Provider shall implement strong password controls on all compatible computing systems (including hand held and mobile devices) that are consistent with the National Institute of Standards and Technology (NIST) Special Publication 800-68 and the SANS Institute Password Protection Policy.

b. The Service Provider shall:
Implement the following security controls on each server, workstation, or portable (e.g., laptop computer) computing device that processes or stores sensitive or confidential information:

i. Install a network-based firewall and/or personal firewalls;

ii. Continuously update anti-virus software on all systems;

iii. Institute a patch-management process including installation of all operating system/software vendor security patches; and

iv. Encrypt all confidential, personal, or sensitive data stored on portable electronic media (including but not limited to CDs and thumb drives) and on computing devices (including but not limited to laptop computers, cell phones, and tablets) with a solution that uses proven industry standard encryption algorithms.

c. The Service Provider shall not:
Transmit confidential, personal, or sensitive data via e-mail or other Internet transport protocol over a public network unless, at minimum, a 128-bit encryption method (for example AES, 3DES, or RC4) and strong passwords are used to secure the data.

d. Mitigation of Harmful Effects. To the extent practicable, Service Provider will mitigate harmful effects known to the Service Provider of a use or disclosure of sensitive and/or confidential information by the Service Provider or its sub-Service Providers.

e. Agents and Contractors or Subcontractors of the Service Provider. To ensure any agent, including a contractor or subcontractor to the Service Provider that provides CCHCS information or created or received by the agent, contractor or subcontractor for the purposes of this contract, Service Provider shall ensure that such agents, contractors or subcontractors comply with the same restrictions and conditions in this ISA that apply to the Service Provider with respect to such information.

f. Notification of Electronic Breach or Improper Disclosure. During the term of this ISA, Service Provider shall notify CCHCS within 24 hours upon discovery of any probable breach of sensitive or confidential information where (1) the information is reasonably believed to have been acquired by an unauthorized person and/or (2) reasonably believed to have an effect of more than 499 people/identities. Immediate notification shall be made to the CCHCS Chief Information Security Officer, Information Security Officer and/or their designee(s). Service Provider shall take prompt corrective action to cure any deficiencies and any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations while at the same time preserving evidence for investigation. Service Provider shall investigate such breach and provide a written report of the investigation to the CCHCS Information Security Officer, postmarked or emailed within eight (8) business days of the discovery of the breach.

g. Employee Training and Discipline. To train and use reasonable measures to ensure compliance with the requirements of this ISA by employees who assist in the performance of functions or activities under this ISA and use or disclose CCHCS information; and have in place a disciplinary process for such employees who intentionally violate any provisions of this ISA, up to and including termination of employment as required by law or policy.

h. Audits, Inspection and Enforcement. From time to time, CCHCS may inspect the facilities, systems, books and records of Service Provider to monitor compliance with this ISA. Service Provider shall promptly remedy any violation of any provision of this ISA and shall certify the same to the CCHCS Information Security Officer in writing The fact that CCHCS

inspects, or fails to inspect, or has the right to inspect, Service Provider's facilities, systems and procedures does not relieve Service Provider of its responsibilities to comply with this ISA. CCHCS's failure to detect or detection, but failure to notify Service Provider or require Service Provider's remediation of any unsatisfactory practice, does not constitute acceptance of such practices or a waiver of CCHCS's enforcement rights under this ISA.

6. Termination

a. Termination for Cause. Upon CCHCS's knowledge of a material breach of this ISA by Service Provider, CCHCS shall either:

i. Provide an opportunity for Service Provider to cure the breach or end the violation and terminate this ISA if Service Provider does not cure the breach or end the violation within the time specified by CCHCS.

ii. Immediately terminate this ISA if Service Provider has breached a material term of this ISA and cure is not possible; or

iii. If neither cure nor termination is feasible, the CCHCS Information Security Officer shall report the violation to the CCHCS Chief Privacy Officer and Director of the CCHCS Legal Office.

b. Judicial or Administrative Proceedings. CCHCS may terminate this ISA, effective immediately, if (i) Service Provider is found liable in a civil matter; or (ii) found guilty in a criminal matter proceeding for a violation of federal or state law, rules and/or regulations, in particular within the nature of information confidentiality and protection.

c. Effect of Termination. Upon termination or expiration of this ISA for any reason, Service Provider shall return or destroy all CCHCS information received from CCHCS that Service Provider still maintains in any form, and shall retain no copies of such information; or, if return or destruction is not feasible, it shall continue to extend the protections of this ISA to such information, and limit further use of such information to those purposes that make the return or destruction of such information infeasible. This provision shall apply to information that is in the possession of contractors to the Service Provider and/or agents of the Service Provider.

EXHIBIT G, ATTACHMENT G-4

Department of State Hospitals' Cases

Involuntary medication of patients housed at state hospitals
(Pen. Code, § 1370)

CONFIDENTIALITY AND INFORMATION SECURITY PROVISIONS

(Revised 10/1/2015)

1. CONFIDENTIALITY AND INFORMATION SECURITY PROVISIONS:

   A. The Contractor shall comply with applicable laws and regulations, including but not limited to Welfare and Institutions Code sections 14100.2 and 5328 et seq., Civil Code section 56 et seq. of the, the Confidentiality of Medical Information Act, Civil Code section 1798 et seq., the Information Practices Act of 1977, Health and Safety Code section 123100 et seq., Patient Access to Health Records Act, Title 42, Code of Federal Regulations (C.F.R.) part 431.300 et seq., and the Health Insurance Portability and Accountability Act (HIPAA), including but not limited to part 1320 d et seq., of Title 42, United States Code and its implementing regulations (including but not limited to Title 45, Code of Federal Regulations, parts 160, 162 and 164 (2013)) ("HIPAA regulations") regarding the confidentiality and security of protected health information (PHI). The following provisions of this Exhibit E, set forth some of the requirements of these statutes and regulations. Exhibit E should not be considered an exclusive list of the requirements. Contractor is required to fulfill the requirements of these statutes and regulations by independently researching and obtaining legal advice on these requirements as they may be amended from time to time. Nothing in this Exhibit suspends OAH's obligations under the California Public Records Act.

2. DEFINITIONS:

   A. The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Covered Entity, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, PHI, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

   B. Specific Definitions

      i. Contractor. Contractor shall generally have the same meaning as the term "business associate" at 45 Code of Federal Regulation, part 160.103 (2013).

ii. HIPAA Rules. HIPAA Rules shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 Code of Federal Regulation, part 160 and Part 164 (2013).

iii. Agreement. Agreement shall be the agreement referenced by the Agreement number set forth on this page's heading.

iv. Personal Information. Personal Information shall have the same meaning as defined in Civil Code section 1798.3, subdivision (c).

3. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE:

A. Contractor agrees to:

i. not use or disclose PHI other than as permitted or required by the Agreement or as required by law,

ii. use appropriate safeguards, and comply with Subpart C of 45 Code of Federal Regulation, part 164 (2013) with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for by the Agreement,

iii. report to the DSH any use or disclosure of PHI not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 Code of Federal Regulations, part 164.410 (2013), and any security incident of which it becomes aware,

iv. in accordance with 45 Code of Federal Regulations, part 164.502(e)(1)(ii) and part 164.308(b)(2) (2013), if applicable ensure that any agents and subcontractors that create, receive, maintain, or transmit PHI on behalf of the Contractor enter into a written agreement with the Contractor agreeing to be bound to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information,

v. make available PHI in a designated record set to the DSH as necessary to satisfy covered entity's obligations under 45 Code of Federal Regulations, part 164.524 (2013) and California Health & Safety Code section 123100,

vi. make any amendment(s) to PHI in a designated record set as directed or agreed to by the covered entity pursuant to 45 Code of Federal Regulations, part 164.526 (2013), or take other measures as necessary to satisfy the covered entity's obligations under 45 Code of Federal Regulations, part 164.526 (2013),

vii. maintain and make available the information required to provide an accounting of disclosures to the DSH as necessary to satisfy covered entity's obligations

under 45 Code of Federal Regulations, part 164.528 (2013),

viii. to the extent the Contractor is to carry out one or more of the DSH's obligation(s) under Subpart E of 45 Code of Federal Regulations, part 164 (2013), comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s) and

ix. make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA regulations.

4. PERMITTED USES AND DISCLOSURES OF PHI BY THE CONTRACTOR:

A. Except as otherwise provided in this Agreement, the Contractor, may use or disclose PHI to perform functions, activities or services identified in this Agreement provided that such use or disclosure would not violate federal or state laws or regulations.

B. The Contractor may not use or disclose the PHI except as provided and permitted or required by the Agreement or required by law.

.

C. Contractor agrees to make uses and disclosures and requests for PHI consistent with the DSH's minimum necessary policies and procedures.

D. Contractor may use and disclose PHI for the proper management and administration of the Contractor or to carry out the legal responsibilities of the Contractor, provided that such uses and disclosures are required by law.

E. Contractor may use PHI to provide data aggregation services related to the health care operations of the DSH. Data aggregation means the combining of PHI created or received by the Contractor for the purposes of this Agreement with PHI received by the Contractor in its capacity as the Contractor of another HIPAA covered entity, to permit data analyses that relate to the health care operations of the DSH.

5. SAFEGUARDS:

A. The Contractor shall develop and maintain an information privacy and security program that includes the implementation of administrative, technical, and physical safeguards appropriate to the size and complexity of the Contractor's operations and the nature and scope of its activities. The information privacy and security program shall reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI that it creates, receives, maintains, or transmits; and prevent

the use or disclosure of PHI other than as provided for by this Agreement. The Contractor shall provide the DSH with information concerning such safeguards as the DSH may reasonably request from time to time.

B. The Contractor shall implement administrative, technical, and physical safeguards to ensure the security of the DSH information on portable electronic media (e.g., floppy disks and CD-ROM) and in paper files. Administrative safeguards to be implemented shall include, but are not limited to training, instructions to employees, and policies and procedures regarding the HIPAA Privacy Rule. Technical safeguards to be implemented must comply with the HIPAA Security Rule and Subpart C of part 164 of the HIPAA regulations with respect to electronic PHI, and shall include, but are not limited to, role-based access, computer passwords, timing out of screens, storing laptop computers in a secure location (never leaving the equipment unattended at workplace, home or in a vehicle) and encryption. Physical safeguards to be implemented shall include, but are not limited to, locks on file cabinets, door locks, partitions, shredders, and confidential destruct.

6. AUTHENTICATION:

A. The Contractor shall implement appropriate authentication methods to ensure information system access to confidential, personal (e.g., PHI) or sensitive data is only granted to properly authenticated and authorized persons. If passwords are used in user authentication (e.g., username/password combination), the Contractor shall implement strong password controls on all compatible computing systems that are consistent with the National Institute of Standards and Technology (NIST) Special Publication 800-68 and the SANS Institute Password Protection Policy.

i. The Contractor shall implement the following security controls on each server, workstation, or portable (e.g., laptop computer) computing device that processes or stores confidential, personal, or sensitive data:·

(1) network-based firewall and/or personal firewall,
(2) continuously updated anti-virus software and
(3) patch-management process including installation of all operating system/software vendor security patches.

ii. Encrypt all confidential, personal, or sensitive data stored on portable electronic media (including, but not limited to, CDs and thumb drives) and on portable computing devices (including, but not limited to, laptop computers, smart phones and PDAs) with a solution that uses proven industry standard algorithms.

iii. Prior to disposal, sanitize all DSH confidential data contained in hard drives, memory devices, portable electronic storage devices, mobile computing

devices, and networking equipment in a manner consistent with the National Institute of Standards and Technology (NIST) Special Publication 800-88.

iv. The Contractor shall not transmit confidential, personal, or sensitive data via e-mail or other Internet transport protocol over a public network unless, at minimum, a 128-bit encryption method (for example AES, 3DES, or RC4) is used to secure the data.

7. MITIGATION OF HARMFUL EFFECTS:

A. Contractor shall mitigate, to the extent practicable, any harmful effect that is known to the Contractor of a use or disclosure of PHI by the Contractor or its subcontractors in violation of the requirements of this Agreement.

8. NOTIFICATION OF BREACH:

A. During the term of this Agreement, Contractor shall report to the DSH any use or disclosure of information not provided for by its contract of which it became aware including breaches of unsecured PHI as required by Section 164.410 of the HIPAA regulations.

9. DISCOVERY OF BREACH:

A. Contractor shall immediately notify the DSH Information Security Officer by telephone call and e-mail upon the discovery of breach of security of PHI in all forms (paper, electronic, or oral) if the PHI was, or is reasonably believed to have been, acquired by an unauthorized person, or within 24 hours by email or fax of the discovery of any suspected security incident, intrusion or unauthorized use or disclosure of PHI in violation of this Agreement, or potential loss of confidential data affecting this Agreement. If the incident occurs after business hours or on a weekend or holiday and involves PHI, notification shall be provided by calling the DSH Information Security Officer. Contractor shall take:

i. prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment and
ii. any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

10. INVESTIGATION OF BREACH:

A. The Contractor shall immediately investigate such security incident, breach, or unauthorized use or disclosure of PHI or confidential data. Within 24 hours of discovery (of the breach), the Contractor shall notify the DSH Information

Security Officer of at least the following:

i. what data elements were involved and the extent of the data involved in the breach,

ii. a description of the unauthorized person(s) known or reasonably believed to have improperly acquired, accessed, used, transmitted, sent or disclosed PHI or confidential data,

iii. a description of where and when the PHI or confidential data is believed to have been improperly acquired, accessed, used, transmitted, sent or disclosed,

iv. a description of the probable causes of the improper acquisition, access, use, transmission, sending or disclosure and

v. whether Civil Code sections 1798.29 (Agency) or 1798.82 (Business) or any other federal or state laws requiring individual notifications of breaches are required.

11. WRITTEN REPORT:

A. The Contractor shall provide a written report of the investigation to the DSH Information Security Officer within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall include, but not be limited to, the information specified above, an estimation of cost for remediation, as well as a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure.

12. NOTIFICATION OF INDIVIDUALS:

A. The Contractor shall notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal law and to pay any costs of such notifications, as well as any costs associated with the breach. Notification shall be made in the most expedient time possible without reasonable delay. The DSH Information Security Officer shall approve the time, manner and content of any such notifications.

13. DSH CONTACT INFORMATION:

A. The Contractor shall direct communications to the DSH Information Security Officer and the Contractor shall initiate contact as indicated herein. The DSH 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 Agreement to which it is incorporated.

Information Security Officer Department of
State Hospitals - Sacramento
1600 9th Street, Room 260
Sacramento, CA 95814
Phone: **REDACTED**
E-mail: **REDACTED**

14. INTERNAL PRACTICES:

A. The Contractor shall make the Contractor's internal practices, books and records relating to the use and disclosure of PHI received from DSH, or created, maintained or received by the Contractor under this Agreement, available to the DSH or to the Secretary of the U.S. Department of Health and Human Services in a time and manner designated by the DSH or by the Secretary, for purposes of determining DSH's compliance with the HIPAA regulations.

15. EMPLOYEE TRAINING AND DISCIPLINE:

A. The Contractor shall train and use reasonable measures to ensure compliance with the requirements of this Agreement by employees who assist in the performance of functions or activities under this Agreement and use or disclose PHI; and discipline such employees who intentionally violate any provisions of this Agreement, including by termination of employment.

16. EFFECT OF TERMINATION:

A. Upon termination or expiration of this Agreement for any reason, the Contractor shall return, at its sole expense, to DSH all health records within five (5) business days or as otherwise specified in the request or notice to return records or, if agreed to by the DSH, destroy all PHI received from DSH or created or received by the Contractor on behalf of the DSH, that the Contractor still maintains in any form. Contractor shall retain no copies of such PHI. However, if return or destruction is not feasible, Contractor shall continue to extend the protections and provisions of this Agreement to such information, and limit further use or disclosure 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 the Contractor, its subcontractor(s), or its agent(s). Notwithstanding this section, OAH shall maintain records in accordance with its approved record retention schedule.

17. MISCELLANEOUS PROVISIONS:

A. The DSH makes no warranty or representation that compliance by the Contractor with this Agreement that the HIPAA regulations shall be adequate or satisfactory for the Contractor's own purposes or that any information in the Contractor's possession or control, or transmitted or received by the Contractor, is or shall be secure from unauthorized use or disclosure. The Contractor is solely responsible for all decisions made by the Contractor regarding the safeguarding of PHI.

B. Assistance in Litigation or Administrative Proceedings. The Contractor shall make itself, and use its best efforts to make any subcontractors, employees or agents assisting the Contractor in the performance of its obligations under this Agreement, available to the DSH at no cost to the DSH to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against the DSH, its directors, officers or employees for claimed violations of HIPAA, regulations or other laws relating to security and privacy based upon actions or inactions of the Contractor and/or its subcontractor, employee, or agent, except where the Contractor or its subcontractor, employee, or agent is a named adverse party.

C. Nothing expressed or implied in the terms and conditions of this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the DSH or the Contractor and their respective successors or assignees, any rights, remedies, obligations or liabilities whatsoever.

D. The terms and conditions in this Agreement shall be interpreted as broadly as necessary to implement and comply with the HIPAA regulations and applicable Federal and State laws. The parties agree that any ambiguity in the terms and conditions of this Agreement shall be resolved in favor of a meaning that complies and is consistent with state and federal law, including HIPAA and the HIPAA regulations.

E. A reference in the terms and conditions of this Agreement to any HIPAA regulation relates to that section in effect or as amended.

F. The obligations of Contractor under this Exhibit E shall survive the termination or expiration of this Agreement.

18. JUDICIAL OR ADMINISTRATIVE PROCEEDINGS:

A. DSH may immediately terminate this Agreement if (a) Contractor is found liable in a civil or criminal proceeding for a violation of the HIPAA Privacy or Security Rule or (b) a finding or stipulation that the Contractor has violated a privacy or security standard or requirement of HIPAA, or other security or privacy laws made in an administrative or civil proceeding in which the Contractor is a party.