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)

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, Section 13400 et seq., Feb. 17, 2009), ("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 Code of Federal Regulations, 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 the applicable requirements of California law governing the exchange, creation, dissemination, maintenance, use or disclosure of PHI that exceeds the requirements of HIPAA, the HITECH Act, and HIPAA Regulations.

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, the HITECH Act, HIPAA Regulations, 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 Code of Federal Regulations 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.

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, HITECH Act, HIPAA Regulations 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 includes 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, HITECH Act, and HIPAA Regulations, 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. ***Lanterman Act*** **–** The "Lanterman Act" means the Lanterman Developmental Disabilities Services Act codified in California Welfare and Institutions Code, Sections 4500, *et seq.*

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 § 160~~0~~4.103~~0~~4, 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 § 164.526(a)~~(2)~~ and 45 CFR § 164.504(e)(2)(ii)(F), 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. Individual requests for amendment(s) are subject to the right of Contractor to exercise denial under 45 CFR § 164.526(a)(2) and under the Lanterman Act. Contractor shall ensure the amendment/s are incorporated into the PHI in accordance with 45 CFR § 164.526.

G. ***Accounting***. Contractor shall provide an accounting of disclosures of PHI to an individual for the six years prior to the date of the individual's request, in accordance with 45 CFR § 164.528 (a)(1), subject to the exceptions listed therein.

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, 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. If there is a contact change of the Privacy Officer, Contractor shall notify DDS

~~and~~ within 10 calendar days ~~of any changes~~ or annually per DDS Technical Bulletin 479.

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 the standards provided by National Institute of Standards and Technology (NIST). 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 all laptops, desktops, tablets, smartphones and other mobile devices, when storing and transmitting electronic PHI, including encryption of ~~that is confidential, sensitive, and 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.).~~when appropriate~~;
5) Requiring the development and maintenance of a Technical Recovery Plan (TRP) documenting the procedures required to restore critical business systems, including conducting an annual performance tabletop test of the TRP and providing annual self-certification of conducting such test to DDS' Information Security Officer; and
6) 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. If there is a contact change of the Security Officer, Contractor shall notify DDS within 10 calendar days or annually per DDS Technical Bulletin 479 ~~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 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)(2)(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 or fax*** 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:

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: 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 presently 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, 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 days. 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, with ~~and~~ DDS's oversight and input, 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. In addition, Contractor, with DDS's input and oversight, shall notify the California Department of Justice, Office of the Attorney General, as required under Civil Code §1898.82.

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 privacy@dds.ca.gov (916) 654-2120	Information Security Officer iso@dds.ca.gov (916) 654-1704
Fax (916) 654-3352	Fax (916) 654-3352

11. *Term and Termination*

A. ***Term.*** The term of this Agreement shall terminate when the regional center's 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 comply with the termination procedure set forth under the Lanterman Act.

~~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.~~

1) DDS may take reasonable steps to provide an opportunity for Contractor to end the violation. If efforts to resolve the problem informally are unsuccessful, DDS shall have the option to issue a letter of noncompliance and establish a Corrective Action Plan ("CAP") under Welfare and Institutions Code, Section 4635; and if Contractor is not in compliance with the CAP, DDS shall move to terminate this Agreement under Welfare and Institutions Code section 4635.
2) If cure is not possible and Contractor has committed a material breach, DDS shall comply with termination provisions set forth in the Lanterman Act to terminate this Agreement and report the violation to the HHS Secretary.

C. ***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 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 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 not feasible, 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. *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 the HITECH Act, HIPAA, HIPAA Regulations, or any more stringent applicable state law protecting PHI in an administrative or civil proceeding in which Contractor is a party.

13. *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.

14. *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.

15. *Employee Training and Discipline*

A. Contractor shall use reasonable measures to ensure compliance with the requirements of this Agreement. In doing so, Contractor shall provide annual security and privacy training on HIPAA to its employees who create, receive, maintain, or transmit PHI or electronic PHI on behalf of Contractor 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.

16. *Audits, Inspection and Enforcement*

From time to time, DDS may inspect the facilities, systems, information security controls, 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':

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).

17. *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, HITECH Act, or any more

stringent applicable state law protecting PHI.

18. *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' 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, the HITECH Act, or other applicable laws. If negotiations are unsuccessful, DDS may move to terminate this Agreement in accordance with the Lanterman Act 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, 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, the HITECH Act, the HIPAA Regulations, 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, the HITECH Act, HIPAA Regulations, 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 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: https://www.hhs.gov/hipaa/index.html
~~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

CONFIDENTIALITY AGREEMENT

Los Angeles County Developmental Services Foundation, Inc. dba Frank D. Lanterman Regional Center

Required for Release of DDS Data
Per the State Administrative Manual Section (5310)

Contractor hereby acknowledges that Department of Developmental Services (DDS) records and documents are subject to strict confidentiality requirements imposed by State and Federal laws including, but not limited to, Health Insurance Portability and Accountability Act 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~~§ 13400 et seq., Feb. 17, 2009), 45 CFR Parts 160 and 164, Sections 56 and following,~~*et seq.*~~ and 1798.24 through 1798.24b of the California Civil Code; California Welfare and Institutions Code, Sections 4514, 5328, and 15633~~00~~ and following ~~et seq~~; California Penal Code Section 11167.5; and any other applicable State or Federal law pertaining to confidentiality.

Contractor assures that the appropriate provisions of both State and Federal law have been met and further assures that all agents of the organization, including subcontractors and agents, understand that unauthorized use, dissemination or distribution of PHI is a crime and that breaches of confidentiality and security may be subject to civil and criminal penalties by the State or Federal government.

Contractor assures that its agents, including subcontractors, will not use, disseminate or otherwise distribute records or documents containing PHI, either on paper or by electronic means, other than as required in the performance of their duties per this contract.

Contractor agrees that unauthorized use, dissemination or distribution of DDS records, documents or information is grounds for immediate termination of any contracts with the DDS and may subject Contractor to penalties, both civil and criminal.

_____ Date: _____
Signature of Contractor's Authorized Representative

_____
Name/Title (Print)

MEDICAID ENROLLMENT REQUIREMENTS

1. PURPOSE

Regional centers coordinate services for consumers for which federal funding is received from the Centers for Medicare and Medicaid Services, and are therefore required to enroll as a Medicaid provider in a manner mutually agreed upon with the State. This exhibit sets forth the terms and conditions under which the Contractor shall enroll as a Medicaid provider.

2. CONTRACT PRACTICES

For the purposes of this Agreement, Contractor agrees to comply with all Medicaid provider enrollment requirements in accordance with Title 42, Code of Federal Regulations (CFR), Sections 455.104 (a), (b)(1)(2)(3)(4), (c), (d), (e); 455.105, (a), (b), (c); 455.106 (a), (b), (c); 455.410; 431.107 (b)(3); 424.302 (d); 424.304 (a)(1); and 424.535 (d)(1).

3. PROCEDURES FOR ENROLLMENT AND RE-ENROLLMENT

Contractor shall adhere to the following enrollment and re-enrollment assurances and procedures:

~~a. Disclosure information for all members of Contractor's Board of Director's:~~

~~1) The name, address, date of birth, and social security number of the board member, as an individual with ownership or control interest. This individual must disclose whether the person (individual or corporation) is related (as a spouse, sibling, parent, or child) to another person with an ownership or control interest.~~

~~2) This individual is subject to a screening process consistent with CFR Section 455.106(a).~~

~~b. Disclosure information for regional center executive director:~~

~~1) The name, address, date of birth, social security number, and driver's license or state identification number of the regional center executive director, as the managing employee of the disclosing entity.~~

~~2) This individual is subject to a screening process consistent with CFR Section 455.106(a).~~

a. Disclosure information required for all members of the Contractor's Board of Directors as well as the Regional Center Executive Director:

1) The name, address, date of birth, and social security number of the board member or Executive Director/Interim Executive Director identified above;

2) If the board member or Executive Director/Interim Executive Director is related to any of the other individuals above (as a spouse, sibling, parent or child);

3) The name of any other enrolled Medicaid provider in which the individual has an ownership or control interest; and

4) The name of any "Excluded Individuals", defined as those that have been placed on either the U.S. Department of Health and Human Services Office of Inspectors' General (OIG) List of Excluded Individuals/Entities or the Department of Health Care Services (DHCS) Medi-Cal Suspended and Ineligible Provider List of persons, or individuals and entities that have been convicted of a criminal offense related to involvement in any program under Medicare, Medicaid or the Title XX services program, or meet the criteria included in Title 17, Section 54311(a)(6).

b. The disclosure information identified in paragraph a. 1) through 4) must be submitted to the State:

1) Upon execution of this contract;

2) Within 35 days of the individuals identified in paragraph a. becoming a member of the Board of Directors or becoming the Regional Center Executive Director/Interim Executive Director;

3) Upon request of the State during revalidation of enrollment requirements every five years or sooner when any of the following circumstances apply:

a) A new Taxpayer Identification (ID) Number is issued by the IRS;
b) There is a cumulative change of 50 percent or more in the person(s) with an ownership or control interest (executive directors or board members) since the information provided in the last complete application package that was approved for enrollment.
c) The two examples above are the most likely circumstances for a regional center to complete a new application, an exhaustive list can be found at Title 22 CCR Section 51000.30. and

c. Individuals that either fail to disclose the required information or meet the "Excluded Individuals" criteria shall be prohibited from serving in the roles identified in paragraph b.