Business Associate Agreement FAQs

Q. What is the Business Associate Agreement?

A. This is an agreement between you and the regional center. It is about how you must protect and keep confidential records you receive or develop when providing Self-Directed Supports. You must comply with federal and state laws, including the federal Health Insurance Portability and Accountability Act (HIPPA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act). These FAQs provide basic information about these requirements. Resources to obtain additional information is found at the end of this document.

Q. What Is Protected Health Information?

A. HIPAA defines Protected Health Information (PHI) as individually identifiable health information you created or received that relates to the past, present or future health needs of an individual. Regional center records that include information about the individual's disability are one example of PHI.

Health information is individually identifiable when it includes a unique identifier that matches a particular individual. Unique identifiers include, but are not limited to: date of birth, unique identification number, address, phone number or email.

Protected health information can be provided in writing, electronically or through a verbal communication. The same requirements to protect PHI apply regardless of how it is shared.

Q. If I provide Self-Directed Supports what are my responsibilities to protect PHI?

A. Your responsibilities fall into three broad categories:

1. You may not use or disclose a consumer's PHI except as allowed by your agreement with the regional center or required by law.

2. You must use appropriate safeguards to prevent the disclosure of a consumer's PHI, including electronic PHI.

3. You must notify the regional center and the Department of Development Services (DDS) of any privacy or security breach.

Q. When can I use or share protected health information?

A. You may only use or share PHI to perform the services you are providing as a Self-Directed Supports vendor. For example, you can share information when a regional center consumer or their legal representative signs a written authorization allowing the information to be shared. Under the Business Associate Agreement, you may also share information with the regional center.

Q. How do I safeguard PHI?

A. You must use appropriate safeguards to protect PHI. Examples of some ways to safeguard information are:

- Records with PHI must be maintained in a secured location;
- PHI can only be used to provide Self-Directed Support services;
- Discussions about PHI should only occur in a secure area, or in a low tone of voice so others do not overhear the discussion;
- Computers and fax machines must be located in a private location.

Q. What are my responsibilities if there is a disclosure of PHI that does not comply with the Business Associate Agreement?

A. You must provide a written notice to the regional center and DDS of any non-compliant disclosure of PHI. The notice must be made without unreasonable delay, and, in no event later than 24 hours after the discovery of the incident.

Q. Where can I get additional information about HIPAA?

To view the entire Security Rule, and for other additional helpful information, see the Centers for Medicare & Medicaid Services (CMS) website.

To view the entire Privacy Rule, and for other additional helpful information, see the Office for Civil Rights (OCR) website.

Vendor Name

Vendor Number

SELF-DETERMINATION PROGRAM: General Self-Directed Supports (099)

BUSINESS ASSOCIATE AGREEMENT / HIPAA

This Business Associate Agreement / HIPAA - Contractor ("**Agreement**"), effective as of 01/01/01, is entered into by Enter name of regional center ("**RC**") and Enter name of contractor ("**Contractor**"). Contractor and the RC are each referred to herein as a "**Party**," and collectively, the "**Parties**." The Parties enter into this Agreement in accordance with the following facts:

A. RC arranges for the provision of services to individuals with developmental disabilities ("**Consumers**"). In providing its services, RC acts as a Business Associate of the California Department of Developmental Services ("**Covered Entity**"). As a necessary part of arranging services to Consumers served by Covered Entity, RC may have access to Protected Health Information ("**PHI**") as such term is defined in the Health Insurance Portability and Accountability Act of 1996, as amended ("**HIPAA**"), and its Privacy and Security Rules.

B. Contractor is, or desires to be, vendored by RC to provide services to or for the benefit of RC's Consumers. Once Contractor is vendored, RC may elect to enter into one or more agreements with Contractor (each, a "**Service Provider Agreement**") to provide specific services to or for the benefit of specific Consumers.

C. Under each Service Provider Agreement, it is anticipated that Contractor may receive and use PHI from and related to RC's Consumers.

D. The purpose of this Agreement is to comply with the requirements of HIPAA, its associated regulations (45 CFR Parts 160-164), and the Health Information Technology for Economic and Clinical Health Act (the "**HITECH Act**"), Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub.L. 111-5), as these laws may be amended, as well as any state law(s) or regulation(s) governing the privacy and security protections of confidential information created or received by Contractor pursuant to each Service Provider Agreement.

In consideration of the following mutual covenants, the Parties therefore agree as follows:

1. **DEFINITIONS**. Except as otherwise defined herein, any and all capitalized terms in this Agreement shall have the definitions set forth in HIPAA and its Privacy and Security Rules.

2. **OBLIGATIONS AND DUTIES OF CONTRACTOR**.

2.1 General. Contractor agrees not to use or disclose any Consumer's PHI other than as permitted or required by this Agreement or by applicable law.

2.2 Safeguard. In accordance with 45 CFR Part 164, Subpart C and 45 CFR §164.314(a)(2)(i)(A)&(B), Contractor agrees to use appropriate administrative, physical and technical safeguards to prevent the use or disclosure of any Consumer's PHI, including Electronic PHI other than as provided for by this Agreement.

2.3 Standard Transactions. Under HIPAA, the US Department of Health and Human Services has adopted certain standard transactions for the electronic exchange of health care data ("**Standard Transactions**"). If Contractor conducts any Standard Transactions on behalf of Covered Entity or RC, Contractor shall comply with the applicable requirements of 45 C.F.R. Parts 160-162. Contractor acknowledges that as of the effective date of this Agreement it may be civilly and/or criminally liable for failure to comply with the safeguards, policies, and procedure requirements, or any of the use and disclosure requirements, established by law.

2.4 Mitigation. Contractor agrees to mitigate, to the extent practicable and appropriate, any harmful effect that is known to Contractor of a use or disclosure of PHI by Contractor in violation of the requirements of this Agreement.

2.5 Agents; Subcontractors. Contractor agrees to ensure that its agents, including any subcontractor, to whom it provides PHI received from, or created or received by Contractor on behalf of Covered Entity or RC, agrees to the same restrictions and conditions applicable to Contractor with respect to such information.

2.6 Access to PHI by Covered Entity, RC or Consumer. Consumers have a right to access their PHI in a designated record set. A "**Designated Record Set**" is defined at 45 CFR 164.501 as a group of records maintained by or for a Covered Entity that comprises the (i) medical records and billing records about Consumers maintained by or for a Covered Entity, (ii) enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan, or (iii) other records that are used, in whole or in part, by or for the Covered Entity to make decisions about Consumers. The term "**record**" means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a Covered Entity. If applicable, and upon request by Covered Entity or RC, Contractor agrees to provide access to Covered Entity, RC or to a Consumer as directed by Covered Entity or RC, the PHI in a Designated Record Set within fifteen (15) days in order to meet the requirements under 45 C.F.R. section 164.524. In addition, as of the effective date of this Agreement, with respect to information contained in an Electronic Health Record, Contractor will provide access to such records in electronic format.

2.7 Amendments to PHI. If applicable, Contractor agrees to make any amendment(s) to PHI in a Designated Record Set as directed or agreed to by Covered Entity or RC pursuant to 45 C.F.R. section 164.526, and as requested by the Covered Entity, RC or a Consumer, within fifteen (15) days of receipt of a request. Any denials,

in whole or in part, of requested amendments shall be made by Contractor in accordance with 45 C.F.R. section 164.526.

2.8 Audit. Contractor agrees that the Secretary of the Department of Health and Human Services (the "**Secretary**") shall have the right to audit Contractor's internal records, books, policies, and practices relating to the use and disclosure of PHI received from, or created or received by Contractor on behalf of Covered Entity or RC, in a time and manner agreed to by the Parties, or as otherwise designated by the Secretary, for purposes of the Secretary determining compliance with the HIPAA Privacy Rule.

2.9 Documentation of Disclosed Information. Contractor agrees to document disclosures of PHI, and information related to such disclosures (collectively, "**Disclosed Information**"), as would be required for Covered Entity or RC to respond to a request by Consumer for an accounting of disclosures of PHI in accordance with 45 C.F.R. section 164.528, as amended from time to time. Contractor hereby agrees to take reasonable steps to enable it to comply with the requirements of this section and to notify RC of any such requests. Contractor shall promptly notify RC of the existence of any Disclosed Information.

2.10 Disclosure Accounting; Retention. Contractor agrees to provide Disclosed Information to Covered Entity, RC or to Consumer at Covered Entity's or RC's request, within fifteen (15) days of such request, in order to permit Covered Entity to meet its obligations in accordance with 45 CFR section 164.528. Contractor shall maintain Disclosed Information for six (6) years following the date of the event or incident to which such information relates.

2.11 Privacy or Security Breach.

2.11.1 In accordance with applicable law, Contractor agrees to give written notice (an "**Incident Notice**") to Covered Entity and RC of any (a) use or disclosure of PHI that is not in compliance with the terms of this Agreement, of which it becomes aware ("**Breach**") and (b) attempted or actual Security Incident (collectively with a Breach, an "**Incident**"). An Incident Notice shall be made without unreasonable delay and, in no event, later than twenty four (24) hours after discovery of such Incident, except where a law enforcement official determines that a notification would impede a criminal investigation or cause damage to national security as described in 45 C.F.R. § 164.412. In addition, an Incident Notice shall include (to the extent possible) the following information:

(a) identification of each Consumer whose Unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed during the Incident;

(b) the circumstances constituting and, to the extent relevant, surrounding the Incident (including, without limitation, the individual(s) causing the Incident and the person(s) receiving or accessing the PHI), the date of the Incident and date of discovery;

(c) the PHI affected or disclosed by the Incident on an individual Consumer-by-individual Consumer basis;

(d) the steps Contractor is taking to investigate and correct the Incident, mitigate harm or loss to affected Consumers, and protect against future similar Incidences,

(e) the actions which Consumers affected by the Incident should take to protect their interests; and

(f) a contact person for additional information.

2.11.2 Contractor shall cooperate with Covered Entity and RC in the investigation of the Incident, and in conducting any risk assessment necessary to determine whether notification of the Incident is required, and shall maintain, and provide at the direction of RC or Covered Entity, all reasonable and appropriate documents, files, records, or logs related to the Incident. For purposes of discovery and reporting of an Incident, Contractor agrees that it shall not be the agent of RC.

2.11.3 To the extent that any Incident involves a Breach of Unsecured PHI, and upon the request of RC or Covered Entity, Contractor shall provide notice to impacted Consumers, the media and the Secretary in the time and manner required by 42 U.S.C. § 17932 and 45 C.F.R. §§ 164.404, 164.406 and 164.408. Prior to providing any such notice, Contractor shall provide RC and Covered Entity with a reasonable opportunity to review and comment on such notice. Contractor shall maintain complete records regarding the Incident, the determination of whether notice is required and the issuance of the notice (including the recipients and content of such notice), and upon request, shall make such records available to RC and Covered Entity. Contractor shall also provide to Consumers affected by the Incident, upon the request of the Covered Entity or RC, such remedies as may be reasonably necessary or appropriate to mitigate the deleterious effects of the Incident including, without limitation, provision of credit report monitoring for a reasonable period of time. Any such remedies provided by Contractor pursuant to this section shall be at the sole expense of Contractor.

2.11.4 Notwithstanding Section 2.11.3 above, if RC or Covered Entity elects to provide the notice referenced in Section 2.11.3, Contractor shall promptly provide to RC and Covered Entity, the information required by 42 U.S.C. § 17932 and 45 C.F.R. §§ 164.404, 164.406 and 164.408, to the extent not previously provided in an Incident Notice.

2.11.5 Any annual notification to the Secretary as required under 42 U.S.C. § 17932(e) and 45 C.F.R. § 164.408(c), shall be provided by Covered Entity or RC, unless Covered Entity or RC directs Contractor to provide such notice within fifteen (15) days after the close of the calendar year. Contractor shall provide RC and Covered Entity a copy of the annual notification before it is provided to the Secretary sufficiently in advance of the due date to permit Covered Entity or RC to revise the notification as may be appropriate.

2.12 Genetic Information. Contractor shall not undertake any activity that may be considered underwriting based on genetic information, as defined by the Genetic Information Nondiscrimination Act and prohibited under the HIPAA Privacy & Security Rules.

2.13 Compliance. Contractor shall comply with all other privacy and security requirements made applicable to it by HIPAA, the HITECH Act and the HITECH Rules as promulgated by the Secretary. In addition, Contractor shall comply at all times with the requirements imposed on Covered Entity, RC and Contractor by state health information privacy laws including, without limitation, the Confidentiality of Medical Information Act (Cal. Civ. Code §56 *et seq*.) and the Lanterman-Petris-Short Act (Cal. Welfare & Inst. Code §5000 *et seq*.)

3. PERMITTED USES AND DISCLOSURES BY CONTRACTOR.

3.1 Business Relationship Activities. Except as otherwise limited in this Agreement, Contractor may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity and RC as specified in the ongoing contractual relationships among the Parties and Covered Entity, provided that such use or disclosure would not violate the HIPAA Privacy Rule or Security Rule if done by Covered Entity, nor violate the minimum necessary policies and procedures of the Covered Entity. For this purpose, the determination of what constitutes the "**minimum necessary**" amount of PHI shall be determined in accordance with 45 C.F.R. section 164.502(b), as amended by section 13405 of the HITECH Act. Without limitation of the foregoing, Contractor shall limit the use, disclosure, or request of PHI, to the extent practicable, to the Limited Data Set (as defined in 45 C.F.R. §164.514(e)(2)) or, if needed by Contractor, to the minimum necessary amount of PHI to satisfy the requirements of each applicable Service Provider Agreement.

3.2 Management and Administration of Contractor. Except as otherwise limited in this Agreement, Contractor may disclose PHI for the proper management and administration of Contractor, provided that disclosures are Required by Law, or Contractor obtains reasonable assurances from the person to whom the information is disclosed that such 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 the person agrees to notify Contractor and RC within one (1) day of discovery of any Incident.

3.3 Data Aggregation. Except as otherwise limited by this Agreement, Contractor may disclose PHI to provide Data Aggregation services to Covered Entity or RC as permitted by 45 CFR 164.504(e)(2)(i)(B). Any aggregated data will be de-identified in compliance with 45 C.F.R. 164.502(d) before it is disclosed. Contractor agrees that it will not disclose any re-identification key or other mechanism to re-identify the data.

3.4 Remuneration. Contractor shall not directly or indirectly receive remuneration in exchange for any PHI unless informed by RC or Covered Entity that

Covered Entity has first obtained a valid authorization from the applicable Consumer that specifically allows PHI to be further exchanged for remuneration by the entity receiving such PHI, or the receipt of such remuneration complies with an otherwise available exception under HIPAA or the HITECH Act.

3.5 Violations of Law. Contractor may use PHI to report violations of law to appropriate federal and state authorities, consistent with 45 CFR 164.502(j)(1).

4. OBLIGATIONS AND DUTIES OF RC.

4.1 Notice of Privacy Practices. RC shall inform Contractor of any limitation(s) in Covered Entity's or RC's notice of privacy practices in accordance with 45 C.F.R. section 164.520, to the extent that such limitation(s), if any, may affect Contractor's use or disclosure of PHI. RC may satisfy this requirement by providing Contractor with the notices of privacy practices that Covered Entity and RC delivers in accordance with 45 C.F.R. section 164.520, as well as any changes to such notice.

4.2 Notice to Consumers of Permission. RC shall notify Contractor of any changes in, or revocation of, permission by a Consumer to use or disclose PHI which RC receives from Covered Entity, to the extent that such changes may affect Contractor's use or disclosure of PHI.

4.3 Notice of Other Restrictions. RC shall notify Contractor of any restriction to the use or disclosure of PHI which RC receives from Covered Entity to which Covered Entity has agreed in accordance with 45 C.F.R. section 164.522, to the extent that such restriction may affect Contractor's use or disclosure of PHI.

4.4 Impermissible Requests. RC shall not request Contractor to use or disclose PHI in any manner that would not be permissible under the HIPAA Privacy Rule if done by RC or Covered Entity.

5. TERM AND TERMINATION.

5.1 General. This Agreement shall remain in effect for so long as RC and Contractor are parties to one or more Service Provider Agreements and shall terminate when all of the PHI provided to Contractor, or created or received by Contractor, is destroyed or returned to RC or Covered Entity. If it is infeasible to return or destroy PHI as set forth above, the terms of this Agreement shall be extended to such PHI in perpetuity, in accordance with the termination provisions set forth below.

5.2 Termination for Cause. RC may terminate this Agreement for cause upon discovery of a material breach by Contractor as follows:

5.2.1 RC shall provide an opportunity for Contractor to cure the breach within ten (10) days from the date RC provides Contractor notice of the breach, or such longer period as may be agreed to by the Parties. If Contractor does not cure the breach within the cure period, then RC may immediately terminate this Agreement and any related Service Provider Agreement(s) in place between the Parties; or

5.2.2 RC may immediately terminate this Agreement, and any related Service Provider Agreement(s) in place between the Parties, if Contractor has breached a material term of this Agreement and cure is not possible; or

5.2.3 If neither termination nor cure is feasible, RC shall report the violation to Covered Entity and the Secretary.

5.3 Return of PHI. Upon termination:

5.3.1 Except as provided in paragraph 5.3.2 of this section, upon termination of this Agreement for any reason, Contractor shall return or destroy all PHI received from Covered Entity or RC, or created or received by Contractor on behalf of Covered Entity or RC. This provision shall apply to PHI that is in the possession of subcontractors or agents of Contractor. Contractor shall retain no copies of the PHI.

5.3.2 If Contractor determines that returning or destroying the PHI is not feasible or practicable, Contractor shall provide to Covered Entity and RC notification of the conditions that make return or destruction impossible or impracticable. Upon such notification, Contractor shall extend the protections of this Agreement to any retained PHI received hereunder and limit any further uses and disclosures to those purposes that make the return or destruction of the information impossible or impracticable for so long as Contractor maintains such PHI.

6. **GENERAL PROVISIONS**.

6.1 Notice. All notices, requests, and other communications given under this Agreement, shall be in writing and deemed duly given: (a) when delivered personally to the recipient; (b) one (1) business day after being sent to the recipient by reputable overnight courier service (charges prepaid); or (c) five (5) business days after being sent by U.S. certified mail (charges prepaid). Except as otherwise provided herein, all notices, requests or communications under this Agreement shall be addressed to the intended recipient as set forth below:

To RC:

RC Name:
RC Address:

To Contractor:

_____
Attention:
_____
_____

6.2 Regulatory References. A reference in this Agreement to any section in the HIPAA Privacy Rule or Security Rule, or the HITECH Act, means the section as presently in effect or as amended.

6.3 Amendment. The Parties agree to take reasonable action to amend this Agreement from time to time as is necessary for all Parties to comply with

the requirements of HIPAA, the HITECH Act, and all related, applicable state and federal laws.

6.4 Survival. The respective rights and obligations of Contractor under Sections 5 and 6 of this Agreement shall survive termination of this Agreement.

6.5 Interpretation. Any ambiguity in this Agreement shall be resolved to permit compliance with the HIPAA Privacy Rule and Security Rule, and the HITECH Act. If there is an inconsistency between the provisions of this Agreement and mandatory provisions of these statutes, the applicable statutory language shall control. Where provisions of this Agreement are different than those mandated by the applicable statutes, but are nonetheless permitted under the law, the provisions of this Agreement shall prevail.

6.6 Rights. Except as expressly stated herein, or the Parties to this Agreement do not intend to create any rights in any third parties, unless such rights are otherwise irrevocably established under HIPAA, or any other applicable law.

6.7 Assignment. No Party may assign its rights and obligations under this Agreement without the prior written consent of the other Party, except both Parties may assign this Agreement to any successors in interest, provided the assignor promptly notifies the other Party of such assignment.

6.8 Independent Parties. Contractor and its agents and employees, in performance of this Agreement, shall act in an independent capacity in the performance of this Agreement and not as officers or employees or agents of RC or Covered Entity. Contractor shall be wholly responsible for the manner in which Contractor and its employees perform the services required of Contractor by the terms of this Agreement. Contractor shall not be, or in any manner represent, imply or hold itself out to be an agent, partner or representative of RC. Contractor has no right or authority to assume or create in writing or otherwise any obligation of any kind, express or implied, for or on behalf of RC. The only relationship between Contractor and RC is that of independent contractors and neither shall be responsible for any obligations, liabilities, or expenses of the other, or any act or omission of the other, except as expressly set forth herein.

6.9 Indemnity. Contractor agrees to indemnify, defend and hold harmless RC and Covered Entity, and their respective employees, directors, officers, agents, subcontractors, or other members of their workforce (collectively, "**Indemnitees**") against all claims, demands, losses, damages or liability of any type or kind whatsoever, arising from or in connection with any breach of this Agreement or of any warranty hereunder or from any negligence or wrongful acts or omissions, including failure to perform its obligations under the Privacy Rule, the Standard Transactions and Code Sets Regulations, the Security Rule, HITECH or other state or federal health information privacy laws by Contractor. Accordingly, on demand, (i) Contractor at his own expense and risk, shall defend any suit, claim, action, legal proceeding, arbitration, or other mediation proceeding (each, an "**Action**"), that may be brought against the Indemnitees or any of them on any such claim or demand as set forth above (the Indemnitees need not have first paid any such claim in order to be so indemnified) and (ii) Contractor shall reimburse Indemnitees for any and all losses, liabilities, lost profits,

fines, penalties, costs or expenses (including reasonable attorneys' fees) that may for any reason be imposed upon Indemnitees as a result of any Action, with counsel reasonably satisfactory to RC. This Section shall survive the expiration or termination of this Agreement for any reason.

6.10 Interpretation; Venue; Jurisdiction. This Agreement shall be construed to comply with the requirements of the HIPAA Rules, and any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules. All other aspects of this Agreement shall be governed under the laws of the State of California. All actions between the Parties shall be venued in the state or district courts of the Enter name of vendoring county .

6.11 Waiver. 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, nor shall such action prohibit enforcement of any obligation on any other occasion.

6.12 Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, the remaining provisions shall remain in full force and effect. In addition, if either Party believes in good faith that any provision of this Agreement fails to comply with the then-current requirements of the HIPAA Privacy Rule or Security Rule, or the HITECH Act, such Party shall notify the other in writing. For a period of up to thirty (30) days, the Parties shall engage in good faith discussions about such concern and, if necessary, amend the terms of this Agreement so that it complies with the law. If the Parties are unable to agree upon the need for amendment, or the amendment itself, then either Party has the right to terminate this Agreement upon 30 days' written notice to the other Party.

6.13 Counterparts; Electronic Copies. This Agreement may be executed in counterparts, each which shall be deemed an original and all of which shall constitute a single instrument. Signed copies of this Agreement delivered by fax or in a PDF email file shall be deemed the same as originals.

Executed at Enter name of city , California, as of the date first set forth above.

RC:

RC Name:
RC Address:

CONTRACTOR:

_____

_____

[*State of Formation and Type of Entity*]

By: _____

Name: _____

Title: _____

Regional Center Executive Director or Designee Signature: