



Contract Number

18-342 A-2

SAP Number

4400008337

Department of Behavioral Health

Department Contract Representative	Ellayna Hoatson
Telephone Number	(909) 388-0858
Contractor	South Coast Community Services
Contractor Representative	Amy Lynn Graves
Telephone Number	(909) 347-9273
Contract Term	July 1, 2018 – June 30 - 2023
Original Contract Amount	\$1,200,000
Amendment Amount	\$300,000
Total Contract Amount	\$1,500,000
Cost Center	9206382200

THIS CONTRACT is entered into in the State of California by and between San Bernardino County, hereinafter called the County, and South Coast Community Services referenced above, hereinafter called Contractor.

IT IS HEREBY AGREED AS FOLLOWS:

WITNESSETH:

IN THAT CERTAIN **Contract No. 18-342** by and between San Bernardino County, a political subdivision of the State of California, and Contractor for Adult Mental Health Clubhouse services, which Contract first became effective July 01, 2018, the following changes are hereby made and agreed to:


- I. ARTICLE IV Funding and Budgetary Restrictions, paragraph I is hereby amended to read as follows:
 - I. The contract amendment amount of \$300,000 shall increase the total contract amount from \$1,200,000 to \$1,500,000 for the contract term.
- II. ARTICLE XIII Duration and Termination, paragraph A is hereby amended to read as follows:
 - A. The term of this Agreement shall be from July 1, 2018 through June 30, 2023 inclusive.
- III. The Schedules A and B for FY 2022/23 will be submitted to, and approved by, the Director or designee at a later date.

- IV. ATTACHMENT I Attestation Regarding Ineligible/Excluded Persons is hereby replaced with revised ATTACHMENT I Attestation Regarding Ineligible/Excluded Persons dated March 2019.
- V. ATTACHMENT II Data Security Requirements is hereby replaced with revised ATTACHMENT II Data Security Requirements dated March 2019.
- VI. All other terms, conditions and covenants in the basic agreement remain in full force and effect.

This Agreement may be executed in any number of counterparts, each of which so executed shall be deemed to be an original, and such counterparts shall together constitute one and the same Agreement. The parties shall be entitled to sign and transmit an electronic signature of this Agreement (whether by facsimile, PDF or other email transmission), which signature shall be binding on the party whose name is contained therein. Each party providing an electronic signature agrees to promptly execute and deliver to the other party an original signed Agreement upon request.

SAN BERNARDINO COUNTY

(Print or type name of corporation, company, contractor, etc.)

By  _____
(Authorized signature - sign in blue ink)

Name _____
(Print or type name of person signing contract)

Title _____
(Print or Type)

Dated: _____

Address _____


 Curt Hagman, Chairman, Board of Supervisors


Dated: _____
 SIGNED AND CERTIFIED THAT A COPY OF THIS DOCUMENT HAS BEEN DELIVERED TO THE CHAIRMAN OF THE BOARD


Lynna Monell
 Clerk of the Board of Supervisors
 of San Bernardino County

By _____
 Deputy

FOR COUNTY USE ONLY

Approved as to Legal Form
 _____
 Dawn Martin, Deputy County Counsel
 Date _____

Reviewed for Contract Compliance
 _____
 Natalie Kessee, Contracts Manager
 Date _____

Reviewed/Approved by Department
 _____
 Georgina Yoshioka, Interim Director
 Date _____

ATTESTATION REGARDING INELIGIBLE/EXCLUDED PERSONS**Contractor South Coast Community Services shall:**

To the extent consistent with the provisions of this Agreement, comply with regulations found in Title 42 Code of Federal Regulations (CFR), Parts 1001 and 1002, et al regarding exclusion from participation in Federal and State funded programs, which provide in pertinent part:

1. Contractor certifies to the following:
 - a. it is not presently excluded from participation in Federal and State funded health care programs,
 - b. there is not an investigation currently being conducted, presently pending or recently concluded by a Federal or State agency which is likely to result in exclusion from any Federal or State funded health care program, and/or
 - c. unlikely to be found by a Federal and State agency to be ineligible to provide goods or services.
2. As the official responsible for the administration of Contractor, the signatory certifies the following:
 - a. all of its officers, employees, agents, sub-contractors and/or persons having five percent (5%) or more of direct or indirect ownership or control interest of the Contractor are not presently excluded from participation in any Federal or State funded health care programs,
 - b. there is not an investigation currently being conducted, presently pending or recently concluded by a Federal or State agency of any such officers, employees, agents and/or sub-contractors which is likely to result in an exclusion from any Federal and State funded health care program, and/or
 - c. its officers, employees, agents and/or sub-contractors are otherwise unlikely to be found by a Federal or State agency to be ineligible to provide goods or services.
3. Contractor certifies it has reviewed, at minimum prior to hire or contract start date and monthly thereafter, the following lists in determining the organization nor its officers, employees, agents, sub-contractors and/or persons having five percent (5%) or more of direct or indirect ownership or control interest of the Contractor are not presently excluded from participation in any Federal or State funded health care programs:
 - a. OIG's List of Excluded Individuals/Entities (LEIE).
 - b. United States General Services Administration's System for Award Management (SAM).
 - c. California Department of Health Care Services Suspended and Ineligible Provider (S&I) List, if receives Medi-Cal reimbursement.
4. Contractor certifies that it shall notify DBH immediately (within 24 hours) by phone and in writing within ten (10) business days of being notified of:
 - a. Any event, including an investigation, that would require Contractor or any of its officers, employees, agents and/or sub-contractors exclusion or suspension under Federal or State funded health care programs, or
 - b. Any suspension or exclusionary action taken by an agency of the Federal or State government against Contractor, or one or more of its officers, employees, agents and/or sub-contractors, barring it or its officers, employees, agents and/or sub-contractors from providing goods or services for which Federal or State funded health care program payment may be made.

Printed name of authorized official

Signature of authorized official

Date

DATA SECURITY REQUIREMENTS

Pursuant to its contract with the State Department of Health Care Services, the Department of Behavioral Health (DBH) requires Contractor adhere to the following data security requirements:

A. Personnel Controls

1. Employee Training. All workforce members who assist in the performance of functions or activities on behalf of DBH, or access or disclose DBH Protected Health Information (PHI) or Personal Information (PI) must complete information privacy and security training, at least annually, at Contractor's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of ten (10) years from the final date of the contract period or from the date of completion of any audit, whichever is later.
2. Employee Discipline. Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.
3. Confidentiality Statement. All persons that will be working with DBH PHI or PI must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The Statement must be signed by the workforce member prior to accessing DBH PHI or PI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for DBH inspection for a period of ten (10) years from the final date of the contract period or from the date of completion of any audit, whichever is later.
4. Background Check. Before a member of the workforce may access DBH PHI or PI, a background screening of that worker must be conducted. The screening should be commensurate with the risk and magnitude of harm the employee could cause, with more thorough screening being done for those employees who are authorized to bypass significant technical and operational security controls. The Contractor shall retain each workforce member's background check documentation for a period of ten (10) years from the final date of the contract period or from the date of completion of any audit, whichever is later.

B. Technical Security Controls

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

6. Patch Management. All workstations, laptops and other systems that process and/or store DBH PHI or PI must have all critical security patches applied with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within thirty (30) days of vendor release. Applications and systems that cannot be patched within this time frame due to significant operational reasons must have compensatory controls implemented to minimize risk until the patches can be installed. Application and systems that cannot be patched must have compensatory controls implemented to minimize risk, where possible.
7. User IDs and Password Controls. All users must be issued a unique user name for accessing DBH PHI or PI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed at least every ninety (90) days, preferably every sixty (60) days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:
 - a. Upper case letters (A-Z)
 - b. Lower case letters (a-z)
 - c. Arabic numerals (0-9)
 - d. Non-alphanumeric characters (special characters)
8. Data Destruction. When no longer needed, all DBH PHI or PI must be wiped using the Gutmann or U.S. Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission of DBH's Office of Information Technology.
9. System Timeout. The system providing access to DBH PHI or PI must provide an automatic timeout, requiring re-authentication of the user session after no more than twenty (20) minutes of inactivity.
10. Warning Banners. All systems providing access to DBH PHI or PI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.
11. System Logging. The system must maintain an automated audit trail which can identify the user or system process which initiates a request for DBH PHI or PI, or which alters DBH PHI or PI. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If DBH PHI or PI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least ten (10) years from the final date of the contract period or from the date of completion of any audit, whichever is later.
12. Access Controls. The system providing access to DBH PHI or PI must use role based access controls for all user authentications, enforcing the principle of least privilege.
13. Transmission Encryption. All data transmissions of DBH PHI or PI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing DBH PHI can be encrypted. This requirement pertains to any type of DBH PHI or PI in motion such as website access, file transfer, and E-Mail.
14. Intrusion Detection. All systems involved in accessing, holding, transporting, and protecting DBH PHI or PI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

C. Audit Controls

1. System Security Review. Contractor must ensure audit control mechanisms that record and examine system activity are in place. All systems processing and/or storing DBH PHI or PI must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.
2. Log Review. All systems processing and/or storing DBH PHI or PI must have a routine procedure in place to review system logs for unauthorized access.
3. Change Control. All systems processing and/or storing DBH PHI or PI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

D. Business Continuity/Disaster Recovery Controls

1. Emergency Mode Operation Plan. Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of DBH PHI or PI held in an electronic format in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than 24 hours.
2. Data Backup Plan. Contractor must have established documented procedures to backup DBH PHI to maintain retrievable exact copies of DBH PHI or PI. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and an estimate of the amount of time needed to restore DBH PHI or PI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of DBH data.

E. Paper Document Controls

1. Supervision of Data. DBH PHI or PI in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. DBH PHI or PI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.
2. Escorting Visitors. Visitors to areas where DBH PHI or PI is contained shall be escorted and DBH PHI or PI shall be kept out of sight while visitors are in the area.
3. Confidential Destruction. DBH PHI or PI must be disposed of through confidential means, such as cross cut shredding and pulverizing.
4. Removal of Data. Only the minimum necessary DBH PHI or PI may be removed from the premises of Contractor except with express written permission of DBH. DBH PHI or PI shall not be considered "removed from the premises" if it is only being transported from one of Contractor's locations to another of Contractor's locations.
5. Faxing. Faxes containing DBH PHI or PI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.
6. Mailing. Mailings containing DBH PHI or PI shall be sealed and secured from damage or inappropriate viewing of such PHI or PI to the extent possible.

Mailings which include 500 or more individually identifiable records of DBH PHI or PI in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of DBH to use another method is obtained.