Medi-Cal Behavioral Health Performance Agreement

between the California Department of Health Care Services and the County of San Diego

STATE OF CALIFORNIA
STANDARD AGREEMENT
STD 213_DHCS (Rev 09/14)

REGISTRATION NUMBER	AGREEMENT NUMBER
	16-93138

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

STATE AGENCY'S NAME (Also known as DHCS, CDHS, DHS or the State)
Department of Health Care Services

CONTRACTOR'S NAME (Also referred to as Contractor)
San Diego County Behavioral Health Division

2. The term of this Agreement is: July 1, 2016 through June 30, 2017

3. The maximum amount of this Agreement is: $ 0 Zero dollars

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

Exhibit A – Program Specifications (including Special Terms and Conditions)	16 pages
Exhibit A – Attachment I – Request for Waiver	1 page
Exhibit B – Funds Provision	1 page
Exhibit C * – General Terms and Conditions	GTC 610
Exhibit D – Information Confidentiality and Security Requirements	7 pages
Exhibit E – Privacy and Information Security Provisions (including Attachment A)	31 pages
Exhibit E – Attachment B – Information Security Exchange Agreement betwee the Social	70 pages

Items shown above with an Asterisk (*), are hereby incorporated by reference and made part of this agreement as if attached hereto.
These documents can be viewed at http://www.dgs.ca.gov/ols/Resources/StandardContractLanguage.aspx

IN WITNESS WHEREOF, this Agreement has been executed by the parties hereto.

CONTRACTOR		California Department of General Services Use Only
CONTRACTOR'S NAME (if other than an individual, state whether a corporation, partnership, etc.) San Diego County Behavioral Health Division		
BY (Authorized Signature) ✍ DHall	DATE SIGNED (Do not type) 9/13/16	
PRINTED NAME AND TITLE OF PERSON SIGNING David Hall, Clerk of the Board of Supervisors		
ADDRESS 3255 Camino Del Rio So. San Diego, CA 92108		
STATE OF CALIFORNIA		
AGENCY NAME Department of Health Care Services		
BY (Authorized Signature) ✍	DATE SIGNED (Do not type)	
PRINTED NAME AND TITLE OF PERSON SIGNING Don Rodriguez, Chief, Contract Management Unit		[X] Exempt per: W&I Code §14703
ADDRESS 1501 Capitol Avenue, Suite 71.5195, MS 1403, P.O. Box 997413, Sacramento, CA 95899-7413		

Approved and/or authorized by the Board of Supervisors of the County of San Diego.
Meeting Date: 7/8/14 Minute Order No. 9
By: _____ Date 9/13/16
Deputy Clerk of the Board Supervisors

APPROVED AS TO FORM AND LEGALITY
COUNTY COUNSEL
BY _____

Exhibit A
Program Specifications

1. Service Overview

The California Department of Health Care Services (hereafter referred to as DHCS or Department) administers the Mental Health Services Act, Projects for Assistance in Transition from Homelessness (PATH) and Community Mental Health Services Grant (MHBG) programs and oversees county provision of community mental health services provided with realignment funds. Contractor (hereafter referred to as County in this Exhibit) must meet certain conditions and requirements to receive funding for these programs and community mental health services. This Agreement, which is County's performance contract, as required by Welfare and Institutions Code (W&I) sections 5650(a), 5651, 5666 5897, and Title 9, California Code of Regulations (CCR), section 3310, sets forth conditions and requirements that County must meet in order to receive this funding. This Agreement does not cover federal financial participation or State general funds as they relate to Medi-Cal services provided through the Mental Health Plan Contracts. County agrees to comply with all of the conditions and requirements described herein.

DHCS shall monitor this Agreement to ensure compliance with applicable federal and State law and applicable regulations. (Government Code sections 11180-11182; W&I §§ 5614, 5651(c), 5717(b), 14124.2(a))

2. Service Location

The services shall be performed at appropriate sites as described in this contract.

3. Service Hours

The services shall be provided during times required by this contract.

4. Project Representatives

A. The project representatives during the term of this Agreement will be:

Department of Health Care Services	**Contractor Name**
Contract Manager: Erika Cristo Telephone: (916) 552-9055 Fax: (916) 440-7620 Email: Erika.Cristo@dhcs.ca.gov	Contract Manager: Alfredo Aguirre, LCSW Telephone: (619) 563-2765 Fax: (619) 563-2775 Email: alfredo.aguirre@sdcounty.ca.gov

B. Direct all inquiries to:

Exhibit A
Program Specifications

Department of Health Care Services	**Contractor's Name**
Mental Health Services Division/Program Policy Unit Attention: Guy Stewart 1500 Capitol Avenue, MS 2702 P.O. Box Number 997413 Sacramento, CA, 95899-7413	Attention: Alfredo Aguirre, LCSW P.O. Box 85524 San Diego, CA 92186-5524
Telephone: (916) 449-5997 Fax: (916) 440-7620 Email: Guy.Stewart@dhcs.ca.gov	Telephone: (619) 563-2765 Fax: (619) 563-2775 Email: alfredo.aguirre@sdcounty.ca.gov

C. Either party may make changes to the information above by giving written notice to the other party. Said changes shall not require an amendment to this Agreement.

5. Services to be Performed

County shall adhere to the program principles and, to the extent funds are available, County shall provide the array of treatment options in accordance with Welfare and Institutions Code sections 5600.2 through 5600.9, inclusive.

A. GENERAL REQUIREMENTS FOR AGREEMENT

County shall comply with all of the requirements in Section A.1 of this Provision for all County mental health programs, including those specified in Sections B, C and D. County shall comply with all of the data and information reporting requirements in Section A.2 for each County mental health program, including those specified in Sections B, C and D of this Provision, for which it receives federal or State funds.

1) W&I section 5651 provides specific assurances, which are listed below, that must be included in this Agreement. County shall:

   a. Comply with the expenditure requirements of W&I Section 17608.05,

   b. Provide services to persons receiving involuntary treatment as required by Part 1 (commencing with Section 5000) and Part 1.5 (commencing with Section 5585) of Division 5 of the Welfare and Institution Code,

   c. Comply with all of the requirements necessary for Medi–Cal reimbursement for mental health treatment services and case management programs provided to Medi-Cal eligible individuals, including, but not limited to, the provisions set forth in Chapter 3 (commencing with Section 5700) of the Welfare and Institutions Code, and submit cost reports and other data to DHCS in the form and manner determined by the DHCS,

Exhibit A
Program Specifications

d. Ensure that the Local Mental Health Advisory Board has reviewed and approved procedures ensuring citizen and professional involvement at all stages of the planning process pursuant to W&I section 5604.2,

e. Comply with all provisions and requirements in law pertaining to patient rights,

f. Comply with all requirements in federal law and regulation pertaining to federally funded mental health programs,

g. Provide all data and information set forth in Sections 5610 and 5664 of the Welfare and Institutions Code,

h. If the County elects to provide the services described in Chapter 2.5 (commencing with Section 5670) of Division 5 of the Welfare and Institution Code, comply with guidelines established for program initiatives outlined in this chapter, and

i. Comply with all applicable laws and regulations for all services delivered, including all laws, regulations, and guidelines of the Mental Health Services Act.

2) County shall comply with all data and information submission requirements specified in this Agreement.

a. County shall provide all applicable data and information required by federal and/or State law in order to receive any funds to pay for its mental health programs and services, including but not limited to its MHSA programs, PATH grant (if the County receives funds from this grant) or MHBG grant. These federal and State laws include, Title 42, United States Code, sections 290cc-21 through 290cc-35 and 300x through 300x-9, inclusive, W&I sections 5610 and 5664 and the regulations that implement, interpret or make specific, these federal and State laws and any DHCS-issued guidelines that relate to the programs or services.

b. County shall comply with the reporting requirements set forth in W&I section 5845(d)(6), Division 1 of Title 9 of the California Code of Regulations (CCR) and any other reporting requirements related to the County's receipt of federal or State funding for mental health programs. County shall submit complete and accurate information to DHCS, and as applicable the Mental Health Services Oversight and Accountability Commission, including, but not limited, to the following:

i. Client and Service Information (CSI) System Data (See Subparagraph c of this Paragraph)

ii. MHSA Quarterly Progress Reports, as specified in Title 9, CCR, section 3530.20. MHSA Quarterly Progress Reports provide the actual number of

Exhibit A
Program Specifications

clients served by MHSA-funded program. Reports are submitted on a quarterly basis.

iii. Full Service Partnership Performance Outcome data, as specified in Title 9, CCR, section 3530.30.

iv. Consumer Perception Survey data, as specified in Title 9, CCR, section 3530.40.

v. The Annual Mental Health Services Act Revenue and Expenditure Report, as specified in W&I section 5899(a) and Title 9, CCR, sections 3510, 3510.010, 3510.020 and DHCS-issued guidelines.

vi. Innovative Project Reports (annual, final and supplements), as specified in title 9, CCR, sections 3580-3580.020.

vii. The Annual Prevention and Early Intervention report, as specified in Title 9, CCR, sections 3560 and 3560.010.

viii. Three Year Program and Evaluation Reports, as specified in Title 9, CCR, sections 3560 and 3560.020.

c. County shall submit CSI data to DHCS, in accordance with the requirements set forth in DHCS' CSI Data Dictionary. County shall:

i. Report monthly CSI data to DHCS within 60 calendar days after the end of the month in which services were provided.

ii. Report within 60 calendar days or be in compliance with an approved plan of correction the DHCS's CSI Unit.

iii. Make diligent efforts to minimize errors on the CSI error file.

iv. Notify DHCS 90 calendar days prior to any change in reporting system and/or change of automated system vendor.

d. In the event that DHCS or County determines that, due to federal or state law changes or business requirements, an amendment is needed of either County's or DHCS' obligations under this contract relating to either DHCS' or County's information needs both DHCS and County agree to provide notice to the other party as soon as practicable prior to implementation. This notice shall include information and comments regarding the anticipated requirements and impacts of the projected changes. DHCS and County agree to meet and discuss the design, development, and costs of the anticipated changes prior to implementation.

Exhibit A
Program Specifications

e. If applicable to a specific federal or State funding source covered by this Agreement, County shall require each of its subcontractors to submit a fiscal year-end cost report to DHCS no later than December 31 following the close of the fiscal year, in accordance with applicable federal and State laws, regulations, and DHCS-issued guidelines.

f. If applicable to a specific federal or State funding source covered by this Agreement, County shall comply with W&I section 5751.7 and ensure that minors are not admitted into inpatient psychiatric treatment with adults. If the health facility does not have specific separate housing arrangements, treatment staff, and treatment programs designed to serve children or adolescents it must request a waiver of this requirement from DHCS as follows:

   i. If this requirement creates an undue hardship on County, County may request a waiver of this requirement. County shall submit the waiver request on Attachment I of this Agreement, to DHCS.

   ii. DHCS shall review County's waiver request and provide a written notice of approval or denial of the waiver. If County's waiver request is denied, County shall comply with the provision of W&I section 5751.7.

   iii. County shall submit, the waiver request to DHCS at the time County submits this Agreement, signed by County, to DHCS for execution. County shall complete Attachment I, including responses to items 1 through 4 and attach it to this Agreement. See Exhibit A, Attachment I, entitled "Request For Waiver" of this Agreement for additional submission information.

   Execution of this Agreement by DHCS shall not constitute approval of a waiver submitted pursuant to this section.

   Any waiver granted in the prior fiscal year's contract shall be deemed to continue until either party chooses to discontinue it. Execution of this contract shall continue independently of the waiver review and approval process.

   iv. In unusual or emergency circumstances, when County needs to request waivers after the annual Performance Contract has been executed, these requests should be sent immediately to: Licensing and Certification Section, Program Oversight and Compliance Branch, California Department of Health Care Services, P.O. Box 997413, MS 2703, Sacramento, CA 95899-7413, Phone: (916) 319-0985.

   v. Each admission of a minor to a facility that has an approved waiver shall be reported to the Local Mental Health Director.

g. If County chooses to participate in the Assisted Outpatient Treatment program (AOT) Demonstration Project Act of 2002 it shall be required to comply with all applicable statutes including, but not limited to, W&I sections 5345 through

5349.5, inclusive. In addition, County shall submit to DHCS any documents that DHCS requests as part of its statutory responsibilities in accordance with DMH Letter No.: 03-01 dated March 20, 2003.

h. For all mental health funding sources received by County that require submission of a cost report, County shall submit a fiscal year-end cost report by December 31st following the close of the fiscal year in accordance with applicable federal and State law, regulations and DHCS-issued guidelines. (W&I section 5705, 9 CCR sections 3500, 3505). The cost report shall be certified as true and correct, by the mental health director and one of the following: the County mental health departments chief financial officer (or equivalent), and individual who has delegated authority to sign for, and reports directly to the county mental health department's chief financial officer (or equivalent), or the county's auditor-controller (or equivalent). Data submitted shall be full and complete. The County shall also submit a reconciled cost report certified by the mental health director and the county's auditor-controller as being true and correct no later than 18 months after the close of the following fiscal year.

If the County does not submit the cost reports by the reporting deadlines or does not meet the other requirements, DHCS shall request a plan of correction with specific timelines (W&I §5897 (d)). If County does not submit cost reports by the reporting deadlines or the County does not meet the other requirements, DHCS may, after a hearing held with no less than 20 days-notice to the county mental health director (W&I § 5655) withhold payments from the MHS Fund until the County is in compliance with W&I section 5664.

B. THE MENTAL HEALTH SERVICES ACT PROGRAM

1) Program Description

Proposition 63, which created the Mental Health Services Act (MHSA), was approved by the voters of California on November 2, 2004. The Mental Health Services (MHS) Fund, which provides funds to counties for the implementation of its MHSA programs, was established pursuant to W&I section 5890. The MHSA was designed to expand California's public mental health programs and services through funding received by a one percent tax on personal incomes in excess of $1 million. Counties use this funding for projects and programs for prevention and early intervention, community services and supports, workforce development and training, innovation, plus capital facilities and technological needs through mental health projects and programs. The State Controller distributes MHS Funds to the counties to plan for and provide mental health programs and other related activities outlined in a county's three-year program and expenditure plan or annual update. MHS Funds are distributed by the State Controller's Office to the counties on a monthly basis.

Exhibit A
Program Specifications

DHCS shall monitor County's use of MHS Funds to ensure that the county meets the MHSA and MHS Fund requirements. (Government Code sections 11180-11182; W&I §§ 5614, 5651(c), 5717(b), 14124.2(a))

2) Issue Resolution Process

County shall have an Issue Resolution Process (Process) to handle client disputes related to the provision of their mental health services. The Process shall be completed in an expedient and appropriate manner. County shall develop a log to record issues submitted as part of the Process. The log shall contain the date the issue was received; a brief synopsis of the issue; the final issue resolution outcome; and the date the final issue resolution was reached.

3) Revenue and Expenditure Report

County shall submit its Revenue and Expenditure Report (RER) by December 31st following the close of the fiscal year in accordance with W&I sections 5705 and 5899, regulations and DHCS-issued guidelines. The RER shall be certified by the mental health director and the County's auditor-controller (or equivalent), using the DHCS-issued certification form. Data submitted shall be full and complete.

If County does not submit the RER by the reporting deadlines or the RER does not meet the requirements, DHCS shall request a plan of correction with specific timelines. (W&I § 5897(d)) If the RER is not timely submitted, or does not meet the requirements, DHCS may, after a hearing held with no less than 20 days- notice to the county mental health director withhold payments from the MHS Fund until the County submits a complete RER. (WIC 5655, 9 CCR 3510(c))

4) Distribution and Use of Local Mental Health Services Funds:

a. W&I section 5891(c) provides that commencing July 1, 2012 on or before the 15th day of each month, pursuant to a methodology provided by DHCS, the State Controller shall distribute to County's Local Mental Health Services Fund (MHS Fund), established by County pursuant to W&I section 5892(f), all unexpended and unreserved funds on deposit as of the last day of the prior month in the Mental Health Services Fund for the provision of specified programs and other related activities.

b. County shall allocate the monthly Local MHS Fund in accordance with W&I section 5892 as follows :

i. Twenty percent of the funds shall be used for prevention and early intervention (PEI) programs in accordance with W&I section 5840. The expenditure for PEI may be increased by County if DHCS determines that the increase will decrease the need and cost for additional services to severely mentally ill persons in County by an amount at least commensurate with the proposed increase.

Exhibit A
Program Specifications

ii. The balance of funds shall be distributed to County's mental health programs for services to persons with severe mental illnesses pursuant to Part 4 of Division 5 of the W&I,(commencing with Section 5850), for the children's system of care and Part 3 of Division 5 of the Welfare and Institutions Code (commencing with Section 5800), for the adult and older adult system of care.

iii. Five percent of the total funding for the County's mental health programs established pursuant to Part 3 of Division 5 of the W&I (commencing with Section 5800), Part 3.6 of Division 5 of the W&I (commencing with Section 5840), and Part 4 of Division 5 of the W&I (commencing with Section 5850) shall be utilized for innovative programs in accordance with W&I sections 5830, 5847 and 5848.

iv. Programs for services pursuant to Part 3 of Division 5 of the W&I (commencing with Section 5800), and Part 4 of Division 5 of the W&I (commencing with Section 5850) may include funds for technological needs and capital facilities, human resource needs, and a prudent reserve to ensure services do not have to be significantly reduced in years in which revenues are below the average of previous years. The total allocation for these purposes shall not exceed 20 percent of the average amount of funds allocated to County for the previous five years.

v. Allocations in Subparagraphs i. through iii. above, include funding for annual planning costs pursuant to W&I section 5848. The total of these costs shall not exceed five percent of the total annual revenues received for the Local MHS Fund. The planning costs shall include moneys for County's mental health programs to pay for the costs of having consumers, family members, and other stakeholders participate in the planning process and for the planning and implementation required for private provider contracts to be significantly expanded to provide additional services.

c. County shall use Local MHS Fund monies to pay for those portions of the mental health programs/services for children and adults for which there is no other source of funds available. (W&I §§ 5813.5(b), 5878.3(a) and 9 CCR 3610(d)).

d. County shall only use Local MHS Funds to expand mental health services. These funds shall not be used to supplant existing state or county funds utilized to provide mental health services. These funds shall only be used to pay for the programs authorized in W&I section 5892. These funds may not be used to pay for any other program and may not be loaned to County's general fund or any other County fund for any purpose. (W&I § 5891(a))

e. All expenditures for County mental health programs shall be consistent with a currently approved three-year program and expenditure plan or annual update pursuant to W&I section 5847. (W&I § 5892(g))

5) Three-Year Program and Expenditure Plan and Annual Updates:

Exhibit A
Program Specifications

a. County shall prepare and submit a three-year program and expenditure plan, and annual updates, adopted by County's Board of Supervisors, to the Mental Health Services Oversight and Accountability Commission (MHSOAC) within 30 calendar days after adoption. (W&I § 5847 (a)) The three-year program and expenditure plan and annual updates shall include all of the following:

   i. A program for Prevention and Early Intervention (PEI) in accordance with Part 3.6 of Division 5 of the Welfare and Institutions Code (commending with Section 5840). (W&I § 5847 (b)(1))

   ii. A program for services to children in accordance with Part 4 of Division 5 of the Welfare and Institutions Code (commencing with Section 5850), to include a wraparound program pursuant to Chapter 4 of Part 6 of Division 9 of the Welfare and Institutions Code (commencing with Section 18250), or provide substantial evidence that it is not feasible to establish a wraparound program in the County. (W&I § 5847 (b)(2))

   iii. A program for services to adults and seniors in accordance with Part 3 of Division 5 of the Welfare and Institutions Code (commencing with Section 5800). (W&I § 5847 (b)(3))

   iv. A program for innovations in accordance with Part 3.2 of Division 5 of the Welfare and Institutions Code (commencing with Section 5830). (W&I § 5847 (b)(4)) Counties shall expend funds for their innovation programs upon approval by the Mental Health Services Oversight and Accountability Commission.

   v. A program for technological needs and capital facilities needed to provide services pursuant to Part 3 of Division 5 of the Welfare and Institutions Code (commencing with Section 5800), Part 3.6 of Division 5 of the Welfare and Institutions Code (commencing with Section 5840), and Part 4 of Division 5 of the Welfare and Institutions Code (commencing with Section 5850). All plans for proposed facilities with restrictive settings shall demonstrate that the needs of the people to be served cannot be met in a less restrictive or more integrated setting. (W&I § 5847 (b)(5))

   vi. Identification of shortages in personnel to provide services pursuant to the above programs and the additional assistance needed from the education and training programs established pursuant to Part 3.1 of Division 5 of the Welfare and Institutions Code (commencing with Section 5820) and Title 9, CCR, section 3830(b). (W&I § 5847 (b)(6))

   vii. Establishment and maintenance of a prudent reserve to ensure the County program will continue to be able to serve children, adults, and seniors that it is currently serving pursuant to Part 3 of Division 5 of the Welfare and Institutions Code (commencing with Section 5800), Part 3.6 of Division 5 of

the Welfare and Institutions Code (commencing with Section 5840), and Part 4 of Division 5 of the Welfare and Institutions Code (commencing with Section 5850), during years in which revenues for the MHS Fund are below recent averages adjusted by changes in the state population and the California Consumer Price Index. (W&I § 5847 (b)(7))

viii. Certification by County's mental health director, which ensures that County has complied with all pertinent regulations, laws, and statutes of the MHSA, including stakeholder participation and non-supplantation requirements. (W&I § 5847 (b)(8))

ix. Certification by County's Mental Health Director and County's Auditor-Controller that the County has complied with any fiscal accountability requirements as directed by DHCS, and that all expenditures are consistent with the requirements of the MHSA. (W&I § 5847 (b)(9))

b. County shall include services in the programs described in Subparagraphs 5.a.i. through 5.a.v., inclusive, to address the needs of transition age youth between the ages of 16 and 25 years old, including the needs of transition age foster youth. (W&I § 5847(c))

c. County shall prepare expenditure plans for the programs described in Subparagraphs 5.a.i. through 5.a.v., inclusive, and annual expenditure updates. Each expenditure plan update shall indicate the number of children, adults, and seniors to be served, and the cost per person. (W&I § 5847(e))

d. County's three-year program and expenditure plan and annual updates shall include reports on the achievement of performance outcomes for services provided pursuant to the Adult and Older Adult Mental Health System of Care Act, Prevention and Early Intervention, and the Children's Mental Health Services Act, which are funded by the MHS Fund and established jointly by DHCS and the MHSOAC, in collaboration with the California Mental Health Director's Association (W&I § 5848(c)) County contracts with providers shall include the performance goals from the County's three-year program and expenditure plan and annual updates that apply to each provider's programs and services.

e. County's three-year program and expenditure plan and annual update shall consider ways to provide services that are similar to those established pursuant to the Mentally Ill Offender Crime Reduction Grant Program. Funds shall not be used to pay for persons incarcerated in state prison or parolees from state prisons. (W&I § 5813.5(f))

6) Planning Requirements and Stakeholder Involvement:

a. County shall develop its three-year program and expenditure plan and annual update with local stakeholders, including adults and seniors with severe mental illness, families of children, adults, and seniors with severe mental illness,

Exhibit A
Program Specifications

providers of services, law enforcement agencies, education, social services agencies, veterans, representatives from veterans organizations, providers of alcohol and drug services, health care organizations, and other important interests. Counties shall demonstrate a partnership with constituents and stakeholders throughout the process that includes meaningful stakeholder involvement on mental health policy, program planning, and implementation, monitoring, quality improvement, evaluation, and budget allocations. County shall prepare and circulate a draft plan and update for review and comment for at least 30 calendar days to representatives of stakeholder interests and any interested party who has requested a copy of the draft plans. (W&I § 5848(a))

b. County's mental health board, established pursuant to W&I section 5604, shall conduct a public hearing on the County's draft three-year program and expenditure plan and annual updates at the close of the 30 calendar day comment period. Each adopted three-year program and expenditure plan or annual update shall summarize and analyze substantive recommendations and describe substantive changes to the three-year program and expenditure plan and annual updates. The County's mental health board shall review the adopted three-year program and expenditure plan and annual updates and make recommendations to County's mental health department for amendments. (W&I § 5848(b) and Title 9, CCR, § 3315)

7) County Requirements for Handling MHSA Funds

a. County shall place all funds received from the State MHS Fund into a Local MHS Fund. The Local MHS Fund balance shall be invested consistent with other County funds and the interest earned on the investments shall be transferred into the Local MHS Fund. (W&I § 5892(f))

b. The earnings on investment of these funds shall be available for distribution from the fund in future years. (W&I § 5892 (f))

c. Other than funds placed in a reserve in accordance with an approved plan, any funds allocated to County which it has not spent for the authorized purpose within the three years shall revert to the State. County may retain MSHA Funds for capital facilities, technological needs, or education and training for up to 10 years before reverting to the State. (W&I § 5892(h))

d. When accounting for all receipts and expenditures of MHSA funds, County must adhere to uniform accounting standards and procedures that conform to the Generally Accepted Accounting Principles (GAAP), as prescribed by the State Controller in Title 2, CCR, Div. 2, Ch. 2, Subchapter 1, Accounting Procedures for Counties, sections 901-949, and a manual, which is currently entitled "Accounting Standards and Procedures for Counties" and available at http://www.sco.ca.gov/pubs_guides.html. (Government Code section 30200)

8) Department Compliance Investigations:

Exhibit A
Program Specifications

DHCS may investigate County's performance of the Mental Health Services Act related provisions of this Agreement and compliance with the provisions of the Mental Health Services Act, and relevant regulations. In conducting such an investigation DHCS may inspect and copy books, records, papers, accounts, documents and any writing as defined by Evidence Code Section 250 that is pertinent or material to the investigation of the County. For purposes of this Paragraph "provider" means any person or entity that provides services, goods, supplies or merchandise, which are directly or indirectly funded pursuant to MHSA. (Gov. Code §§ 11180, 11181, 11182 and W&I Code § 14124.2)

9) County Breach, Plan of Correction and Withholding of State Mental Health Funds:

a. If DHCS determines that County is out-of-compliance with the Mental Health Services Act related provisions of this Agreement, DHCS may request that County submit a plan of correction, including a specific timeline to correct the deficiencies, to DHCS. (W&I § 5897(d))

b. In accordance with Welfare and Institutions Code Section 5655, if DHCS considers County to be substantially out-of-compliance with any provision of the Mental Health Services Act or relevant regulations, including all reporting requirements, the director shall order County to appear at a hearing before the Director or the Director's designee to show cause why the Department should not take administrative action. County shall be given at least twenty (20) days notice before the hearing.

c. If the Director determines that there is or has been a failure, in a substantial manner, on the part of County to comply with any provision of the W&I code or its implementing regulations, and that administrative sanctions are necessary, the Department may invoke any, or any combination of, the following sanctions:

1) Withhold part or all state mental health funds from County.

2) Require County to enter into negotiations with DHCS to agree on a plan for County to address County's non-compliance. (W&I § 5655.)

C. PROJECTS FOR ASSISTANCE IN TRANSITION FROM HOMELESSNESS (PATH) PROGRAM (Title 42, United States Code, sections 290cc-21 through 290cc-35, inclusive)

Pursuant to Title 42, United State Code, sections 290cc-21 through 290cc-35, inclusive, the State of California has been awarded federal homeless funds through the federal McKinney Projects for Assistance in Transition from Homelessness (PATH) formula grant. The PATH grant funds community based outreach, mental health and substance abuse referral/treatment, case management and other support services, as well as a limited set of housing services for the homeless mentally ill.

Exhibit A
Program Specifications

While county mental health programs serve thousands of homeless persons with realignment funds and other local revenues, the PATH grant augments these programs by providing services to approximately 8,300 additional persons annually. The county determines its use of PATH funds based on county priorities and needs.

If County wants to receive PATH funds, it shall submit its Request for Application (RFA) responses and required documentation specified in DHCS' RFA. County shall complete its RFA responses in accordance with the instructions, enclosures and attachments available on the DHCS website at: http://www.dhcs.ca.gov/services/MH/Pages/PATH.aspx.

If County applied for and DHCS approved its request to receive PATH grant funds, the RFA, County's RFA responses and required documentation, and DHCS' approval constitute provisions of this Agreement and are incorporated by reference herein. County shall comply with all provisions of the RFA and the County's RFA responses in order to receive its PATH grant funds.

D. COMMUNITY MENTAL HEALTH SERVICES GRANT (MHBG) PROGRAM (Title 42, United States Code section 300x-1 et seq.)

DHCS awards federal Community Mental Health Services Block Grant funds (known as Mental Health Block Grant (MHBG)) to counties in California. The county mental health agencies provide a broad array of mental health services within their mental health system of care (SOC) programs. These programs provide services to the following target populations: children and youth with serious emotional disturbances (SED) and adults and older adults with serious mental illnesses (SMI).

The MHBG funds provide the counties with a stable, flexible, and non-categorical funding base that the counties can use to develop innovative programs or augment existing programs within their SOC. The MHBG funds also assist the counties in providing an appropriate level of community mental health services to the most needy individuals in the target populations who have a mental health diagnosis, and/or individuals who have a mental health diagnosis with a co-occurring substance abuse disorder.

If County wants to receive MHBG funds, it shall submit its RFA responses and required documentation specified in DHCS' RFA. County shall complete its RFA responses in accordance with the instructions, enclosures and attachments available on the DHCS website at: http://www.dhcs.ca.gov/services/MH/Pages/MHBG.aspx.

If County applied for and DHCS approved its request to receive MHBG grant funds, the RFA, County's RFA responses and required documentation, and DHCS' approval constitute provisions of this Agreement and are incorporated by reference herein. County shall comply with all provisions of the RFA and the County's RFA responses in order to receive its MHBG grant funds.

Exhibit A
Program Specifications

E. SPECIAL TERMS AND CONDITIONS

1. Audit and Record Retention

(Applicable to agreements in excess of $10,000)

a. County and/or Subcontractor(s) shall maintain books, records, documents, and other evidence, accounting procedures and practices, sufficient to properly support all direct and indirect costs of whatever nature claimed to have been incurred in the performance of this Agreement, including any matching costs and expenses. The forgoing constitutes "records" for the purpose of this provision.

b. County's and/or Subcontractor's facility or office or such part thereof as may be engaged in the performance of this Agreement and his/her records shall be subject at all reasonable times to inspection, audit, and reproduction.

c. County agrees that DHCS, the Department of General Services, the Bureau of State Audits, or their designated representatives including the Comptroller General of the United States shall have the right to review and copy any records and supporting documentation pertaining to the performance of this Agreement. County agrees to allow the auditor(s) access to such records during normal business hours and to allow interviews of any employees who might reasonably have information related to such records. Further, County agrees to include a similar right of the State to audit records and interview staff in any subcontract related to performance of this Agreement.

d. County and/or Subcontractor(s) shall preserve and make available his/her records (1) for a period of three years from the date of final payment under this Agreement, and (2) for such longer period, if any, as is required by applicable statute, by any other provision of this Agreement, or by subparagraphs (1) or (2) below.

    1) If this Agreement is completely or partially terminated, the records relating to the work terminated shall be preserved and made available for a period of three years from the date of any resulting final settlement.

    2) If any litigation, claim, negotiation, audit, or other action involving the records has been started before the expiration of the three-year period, the records shall be retained until completion of the action and resolution of all issues which arise from it, or until the end of the regular three-year period, whichever is later.

e. County and/or Subcontractor(s) shall comply with the above requirements and be aware of the penalties for violations of fraud and for obstruction of investigation as set forth in Public Contract Code § 10115.10, if applicable.

f. County and/or Subcontractor(s) may, at its discretion, following receipt of final payment under this Agreement, reduce its accounts, books, and records related to this Agreement to microfilm, computer disk, CD ROM, DVD, or other data storage medium. Upon request by an authorized representative to inspect, audit or obtain copies of said records, County and/or Subcontractor(s) must supply or make available applicable devices, hardware, and/or software necessary to view, copy, and/or print said records. Applicable devices may include, but are not limited to, microfilm readers and microfilm printers, etc.

Exhibit A
Program Specifications

g. County shall, if applicable, comply with the Single Audit Act and the audit reporting requirements set forth in OMB Circular A-133.

2. **Dispute Resolution Process**

a. A Contractor/County grievance exists whenever there is a dispute arising from DHCS' action in the administration of an Agreement. If there is a dispute or grievance between County and DHCS, County must seek resolution using the procedure outlined below.
   1) County should first informally discuss the problem with the DHCS Program Contract Manager. If the problem cannot be resolved informally, County shall direct its grievance together with any evidence, in writing, to the program Branch Chief. The grievance shall state the issues in dispute, the legal authority or other basis for County's position and the remedy sought. The Branch Chief shall render a decision within ten (10) working days after receipt of the written grievance from County. The Branch Chief shall respond in writing to County indicating the decision and reasons therefore. If County disagrees with the Branch Chief's decision, County may submit an appeal to the second level.
   2) When appealing to the second level, County must prepare an appeal indicating the reasons for disagreement with Branch Chief's decision. The County shall include a copy of the County's original statement of dispute along with any supporting evidence and a copy of the Branch Chief's decision. The appeal shall be addressed to the Deputy Director of the division in which the branch is organized within ten (10) working days from receipt of the Branch Chief's decision. The Deputy Director of the division in which the branch in organized or his/her designee shall meet with County to review the issues raised. A written decision signed by the Deputy Director of the division in which the branch is organized or his/her designee shall be directed to County within twenty (20) working days of receipt of the County's second level appeal.

b. If County wishes to appeal the decision of the Deputy Director of the division in which the branch is organized or his/her designee, County shall follow the procedures set forth in Health and Safety Code Section 100171.

c. Unless otherwise stipulated in writing by DHCS, all dispute, grievance and/or appeal correspondence shall be directed to the DHCS Program Contract Manager.

d. There are organizational differences within DHCS' funding programs and the management levels identified in this dispute resolution provision may not apply in every contractual situation. When a grievance is received and organizational differences exist, County shall be notified in writing by the DHCS Program Contract Manager of the level, name, and/or title of the appropriate management official that is responsible for issuing a decision.

3. **Novation**

Exhibit A
Program Specifications

a. If County proposes any novation agreement, DHCS shall act upon the proposal within 60 days after receipt of the written proposal. DHCS may review and consider the proposal, consult and negotiate with County, and accept or reject all or part of the proposal. Acceptance or rejection of the proposal may be made orally within the 60-day period and confirmed in writing within five days of said decision. Upon written acceptance of the proposal, DHCS will initiate an amendment to this Agreement to formally implement the approved proposal.

Exhibit A, Attachment I
Request for Waiver

Request for Waiver Pursuant To Section 5751.7 of the Welfare and Institutions Codes

_____ hereby requests a waiver for the following public or private health facilities pursuant to Section 5751.7 of the Welfare and Institutions Code for the term of this contract. These are facilities where minors may be provided psychiatric treatment with nonspecific separate housing arrangements, treatment staff, and treatment programs designed to serve minors. However, no minor shall be admitted for psychiatric treatment into the same treatment ward as an adult receiving treatment who is in the custody of any jailor for a violent crime, is a known registered sex offender, or has a known history of, or exhibits inappropriate sexual or other violent behavior which would present a threat to the physical safety of others.

The request for waiver must include, as an attachment, the following:

1. A description of the hardship to the County/City due to inadequate or unavailable alternative resources that would be caused by compliance with the state policy regarding the provision of psychiatric treatment to minors.

2. The specific treatment protocols and administrative procedures established by the County/City for identifying and providing appropriate treatment to minors admitted with adults.

3. Name, address, and telephone number of the facility

   - Number of the facility's beds designated for involuntary treatment
   - Type of facility, license(s), and certification(s) held (including licensing and certifying agency and license and certificate number)
   - A copy of the facility's current license or certificate and description of the program, including target population and age groups to be admitted to the designated facility.

4. The County Board of Supervisors' decision to designate a facility as a facility for evaluation and treatment pursuant to Welfare and Institutions Codes 5150, 5585.50, and 5585.55.

Execution of this Agreement shall not constitute approval of this waiver. Full execution of this contract will continue independently of the waiver review and approval process.

Any waiver granted in the prior fiscal year's Agreement shall be deemed to continue until either party chooses to discontinue it.

To rescind the county's designation of a designated facility, the county shall send a letter to the Department on official letterhead signed by the County Behavioral Health Director or his or her designee indicating that the county no longer designates the particular facility. If not otherwise specified by the host county in the letter to the Department, the discontinuance shall be effective the date the letter to the Department is postmarked and the facility shall no longer be approved as a designated facility as of this date.

Exhibit B
Funds Provision

1. Budget Contingency Clause

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

B. If funding for any fiscal year is reduced or deleted by the Budget Act for purposes of this program, DHCS shall have the option to either cancel this Agreement with no liability occurring to DHCS, or offer an agreement amendment to San Diego County Behavioral Health Division to reflect the reduced amount.

Exhibit D

Information Confidentiality and Security Requirements

1. **Definitions**. For purposes of this Exhibit, the following definitions shall apply:

   A. **Public Information:** Information that is not exempt from disclosure under the provisions of the California Public Records Act (Government Code sections 6250-6265) or other applicable state or federal laws.

   B. **Confidential Information:** Information that is exempt from disclosure under the provisions of the California Public Records Act (Government Code sections 6250-6265) or other applicable state or federal laws.

   C. **Sensitive Information:** Information that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion. Sensitive Information may be either Public Information or Confidential Information. It is information that requires a higher than normal assurance of accuracy and completeness. Thus, the key factor for Sensitive Information is that of integrity. Typically, Sensitive Information includes records of agency financial transactions and regulatory actions.

   D. **Personal Information:** Information that identifies or describes an individual, including, but not limited to, their name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. **It is DHCS' policy to consider all information about individuals private unless such information is determined to be a public record.** This information must be protected from inappropriate access, use, or disclosure and must be made accessible to data subjects upon request. Personal Information includes the following:

   Notice-triggering Personal Information: Specific items of personal information (name plus Social Security number, driver license/California identification card number, or financial account number) that may trigger a requirement to notify individuals if it is acquired by an unauthorized person. For purposes of this provision, identity shall include, but not be limited to name, identifying number, symbol, or other identifying particular assigned to the individual, such as finger or voice print or a photograph. See Civil Code sections 1798.29 and 1798.82.

2. **Nondisclosure**. The Contractor and its employees, agents, or subcontractors shall protect from unauthorized disclosure any Personal Information, Sensitive Information, or Confidential Information (hereinafter identified as PSCI).

3. The Contractor and its employees, agents, or subcontractors shall not use any PSCI for any purpose other than carrying out the Contractor's obligations under this Agreement.

4. The Contractor and its employees, agents, or subcontractors shall promptly transmit to the DHCS Program Contract Manager all requests for disclosure of any PSCI not emanating from the person who is the subject of PSCI.

5. The Contractor shall not disclose, except as otherwise specifically permitted by this Agreement or authorized by the person who is the subject of PSCI, any PSCI to anyone other than DHCS without prior written authorization from the DHCS Program Contract Manager, except if disclosure is required by State or Federal law.

Exhibit D
Information Confidentiality and Security Requirements

6. The Contractor shall observe the following requirements:

   A. Safeguards. The Contractor shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PSCI, including electronic PSCI that it creates, receives, maintains, uses, or transmits on behalf of DHCS. 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 the Contractor's operations and the nature and scope of its activities, Including at a minimum the following safeguards:

   1) Personnel Controls

   a. ***Employee Training.*** All workforce members who assist in the performance of functions or activities on behalf of DHCS, or access or disclose DHCS PSCI, must complete information privacy and security training, at least annually, at Business Associate's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following contract termination.

   b. ***Employee Discipline.*** Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.

   c. ***Confidentiality Statement.*** All persons that will be working with DHCS PHI or PI must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to DHCS PHI or PI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for DHCS inspection for a period of six (6) years following contract termination.

   d. ***Background Check.*** Before a member of the workforce may access DHCS PHI or PI, a thorough background check of that worker must be conducted, with evaluation of the results to assure that there is no indication that the worker may present a risk to the security or integrity of confidential data or a risk for theft or misuse of confidential data. The Contractor shall retain each workforce member's background check documentation for a period of three (3) years following contract termination.

   2) Technical Security Controls

   a. ***Workstation/Laptop encryption.*** All workstations and laptops that process and/or store DHCS PHI or PI must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the DHCS Information Security Office.
   b. ***Server Security.*** Servers containing unencrypted DHCS 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.

Exhibit D
Information Confidentiality and Security Requirements

c. ***Minimum Necessary.*** Only the minimum necessary amount of DHCS PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.

d. ***Removable media devices.*** All electronic files that contain DHCS PHI or PI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, smartphones, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.

e. ***Antivirus software.*** All workstations, laptops and other systems that process and/or store DHCS PHI or PI must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

f. ***Patch Management.*** All workstations, laptops and other systems that process and/or store DHCS PHI or PI must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release.

g. ***User IDs and Password Controls.*** All users must be issued a unique user name for accessing DHCS PHI or PI. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within 24 hours. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every 90 days, preferably every 60 days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:

- Upper case letters (A-Z)
- Lower case letters (a-z)
- Arabic numerals (0-9)
- Non-alphanumeric characters (punctuation symbols)

h. ***Data Destruction.*** When no longer needed, all DHCS PHI or PI must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the PHI or PI cannot be retrieved.

i. ***System Timeout.*** The system providing access to DHCS PHI or PI must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.

j. ***Warning Banners.*** All systems providing access to DHCS PHI or PI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.

k. ***System Logging.*** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for DHCS PHI or PI, or which alters DHCS 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

Exhibit D
Information Confidentiality and Security Requirements

DHCS PHI or PI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.

l. ***Access Controls.*** The system providing access to DHCS PHI or PI must use role based access controls for all user authentications, enforcing the principle of least privilege.

m. ***Transmission encryption.*** All data transmissions of DHCS PHI or PI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing PHI can be encrypted. This requirement pertains to any type of PHI or PI in motion such as website access, file transfer, and E-Mail.

n. ***Intrusion Detection.*** All systems involved in accessing, holding, transporting, and protecting DHCS PHI or PI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

3) Audit Controls

a. ***System Security Review.*** All systems processing and/or storing DHCS PHI or PI must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.

b. ***Log Reviews.*** All systems processing and/or storing DHCS PHI or PI must have a routine procedure in place to review system logs for unauthorized access.

c. ***Change Control.*** All systems processing and/or storing DHCS PHI or PI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

4) Business Continuity / Disaster Recovery Controls

a. ***Emergency Mode Operation Plan.*** Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic DHCS PHI or PI in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than 24 hours.

b. ***Data Backup Plan.*** Contractor must have established documented procedures to backup DHCS PHI to maintain retrievable exact copies of DHCS 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 DHCS PHI or PI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of DHCS data.

5) Paper Document Controls

a. ***Supervision of Data.*** DHCS 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

Exhibit D
Information Confidentiality and Security Requirements

information is not being observed by an employee authorized to access the information. DHCS PHI or PI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

b. ***Escorting Visitors.*** Visitors to areas where DHCS PHI or PI is contained shall be escorted and DHCS PHI or PI shall be kept out of sight while visitors are in the area.

c. ***Confidential Destruction.*** DHCS PHI or PI must be disposed of through confidential means, such as cross cut shredding and pulverizing.

d. ***Removal of Data.*** DHCS PHI or PI must not be removed from the premises of the Contractor except with express written permission of DHCS.

e. ***Faxing.*** Faxes containing DHCS PHI or PI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.

f. ***Mailing.*** Mailings of DHCS PHI or PI shall be sealed and secured from damage or inappropriate viewing of PHI or PI to the extent possible. Mailings which include 500 or more individually identifiable records of DHCS 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 DHCS to use another method is obtained.

B. ***Security Officer.*** The Contractor shall designate a Security Officer to oversee its data security program who will be responsible for carrying out its privacy and security programs and for communicating on security matters with DHCS.

Discovery and Notification of Breach. Notice to DHCS:

(1) To notify DHCS **immediately** upon the discovery of a suspected security incident that involves data provided to DHCS by the Social Security Administration. This notification will be **by telephone call plus email or fax** upon the discovery of the breach. (2) To notify DHCS **within 24 hours by email or fax** of the discovery of unsecured PHI or PI in electronic media or in any other media if the PHI or PI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, any suspected security incident, intrusion or unauthorized access, use or disclosure of PHI or PI in violation of this Agreement and this Addendum, or potential loss of confidential data affecting this Agreement. A breach shall be treated as discovered by the contractor as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of the contractor..

Notice shall be provided to the DHCS Program Contract Manager, the DHCS Privacy Officer and the DHCS Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves data provided to DHCS by the Social Security Administration, notice shall be provided by calling the DHCS EITS Service Desk. Notice shall be made using the "DHCS Privacy Incident Report" form, including all information known at the time. The contractor shall use the most current version of this form, which is posted on the DHCS Privacy Office website (www.dhcs.ca.gov, then select "Privacy" in the left column and then

Exhibit D
Information Confidentiality and Security Requirements

"Business Use" near the middle of the page) or use this link: http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/DHCSBusinessAssociatesOnly.aspx

C. Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of PHI or PI, the Contractor shall take:
   1) Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment and
   2) Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

D. ***Investigation of Breach.*** The Contractor shall immediately investigate such security incident, breach, or unauthorized use or disclosure of PSCI. If the initial report did not include all of the requested information marked with an asterisk, then within seventy-two (72) hours of the discovery, The Contractor shall submit an updated "DHCS Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer:

E. ***Written Report.*** The Contractor shall provide a written report of the investigation to the DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer, if all of the required information was not included in the DHCS Privacy Incident Report, within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall include, but not be limited to, the information specified above, as well as a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure.

F. ***Notification of Individuals.*** The Contractor shall notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal law and shall pay any costs of such notifications, as well as any costs associated with the breach. The DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer shall approve the time, manner and content of any such notifications.

7. **Affect on lower tier transactions.** The terms of this Exhibit shall apply to all contracts, subcontracts, and subawards, regardless of whether they are for the acquisition of services, goods, or commodities. The Contractor shall incorporate the contents of this Exhibit into each subcontract or subaward to its agents, subcontractors, or independent consultants.

8. **Contact Information.** To direct communications to the above referenced DHCS staff, the Contractor shall initiate contact as indicated herein. DHCS 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 Exhibit or the Agreement to which it is incorporated.

DHCS Program Contract Manager	DHCS Privacy Officer	DHCS Information Security Officer

Exhibit D
Information Confidentiality and Security Requirements

See the Scope of Work exhibit for Program Contract Manager information	Privacy Officer c/o Office of Legal Services Department of Health Care Services P.O. Box 997413, MS 0011 Sacramento, CA 95899-7413 Email: privacyofficer@dhcs.ca.gov Telephone: (916) 445-4646	Information Security Officer DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95899-7413 Email: iso@dhcs.ca.gov Telephone: ITSD Help Desk (916) 440-7000 or (800) 579-0874

9. **Audits and Inspections.** From time to time, DHCS may inspect the facilities, systems, books and records of the Contractor to monitor compliance with the safeguards required in the Information Confidentiality and Security Requirements (ICSR) exhibit. Contractor shall promptly remedy any violation of any provision of this ICSR exhibit. The fact that DHCS 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 ICSR exhibit.

EXHIBIT E

PRIVACY AND INFORMATION SECURITY PROVISIONS

This Exhibit E is intended to protect the privacy and security of specified Department information that Contractor may access, receive, or transmit under this Agreement. The Department information covered under this Exhibit E consists of: (1) Protected Health Information as defined under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA")(PHI): and (2) Personal Information (PI) as defined under the California Information Practices Act (CIPA), at California Civil Code Section 1798.3. Personal Information may include data provided to the Department by the Social Security Administration.

Exhibit E consists of the following parts:

1. Exhibit E-1, HIPAA Business Associate Addendum, which provides for the privacy and security of PHI.

2. Exhibit E-2, which provides for the privacy and security of PI in accordance with specified provisions of the Agreement between the Department and the Social Security Administration, known as the Information Exchange Agreement (IEA) and the Computer Matching and Privacy Protection Act Agreement between the Social Security Administration and the California Health and Human Services Agency (Computer Agreement) to the extent Contractor access, receives, or transmits PI under these Agreements. Exhibit E-2 further provides for the privacy and security of PI under Civil Code Section 1798.3(a) and 1798.29.

3. Exhibit E-3, Miscellaneous Provision, sets forth additional terms and conditions that extend to the provisions of Exhibit E in its entirety.

EXHIBIT E-1

HIPAA Business Associate Addendum

1. Recitals.

A. A business associate relationship under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("the HITECH Act"), 42 U.S.C. Section 17921 et seq., and their implementing privacy and security regulations at 45 CFR Parts 160 and 164 ("the HIPAA regulations") between Department and Contractor arises only to the extent that Contractor creates, receives, maintains, transmits, uses or discloses PHI or ePHI on the Department's behalf, or provides services, arranges, performs or assists in the performance of functions or activities on behalf of the Department that are included in the definition of "business associate" in 45 C.F.R. 160.103 where the provision of the service involves the disclosure of PHI or ePHI from the Department, including but not limited to, utilization review, quality assurance, or benefit management. To the extent Contractor performs these services, functions, and activities on behalf of Department, Contractor is the Business Associate of the Department, acting on the Department's behalf. The Department and Contractor are each a party to this Agreement and are collectively referred to as the "parties."

B. The Department wishes to disclose to Contractor certain information pursuant to the terms of this Agreement, some of which may constitute Protected Health Information ("PHI"), including protected health information in electronic media ("ePHI"), under federal law, to be used or disclosed in the course of providing services and activities as set forth in Section 1.A. of Exhibit E-1 of this Agreement. This information is hereafter referred to as "Department PHI".

C. The purpose of this Exhibit E-1 is to protect the privacy and security of the PHI and ePHI that may be created, received, maintained, transmitted, used or disclosed pursuant to this Agreement, and to comply with certain standards and requirements of HIPAA, the HITECH Act, and the HIPAA regulations, including, but not limited to, the requirement that the Department must enter into a contract containing specific requirements with Contractor prior to the disclosure of PHI to

Contractor, as set forth in 45 CFR Parts 160 and 164 and the HITECH Act. To the extent that data is both PHI or ePHI and Personally Identifying Information, both Exhibit E-2 (including Attachment B, the SSA Agreement between SSA, CHHS and DHCS, referred to in Exhibit E-2) and this Exhibit E-1 shall apply.

D. The terms used in this Exhibit E-1, but not otherwise defined, shall have the same meanings as those terms have in the HIPAA regulations. Any reference to statutory or regulatory language shall be to such language as in effect or as amended.

2. Definitions.

A. Breach shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.

B. Business Associate shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.

C. Covered Entity shall have the meaning given to such term under HIPAA, the HITECH Act, and the HIPAA regulations.

D. Department PHI shall mean Protected Health Information or Electronic Protected Health Information, as defined below, accessed by Contractor in a database maintained by the Department, received by Contractor from the Department or acquired or created by Contractor in connection with performing the functions, activities and services on behalf of the Department as specified in Section 1.A. of Exhibit E-1 of this Agreement. The terms PHI as used in this document shall mean Department PHI.

E. Electronic Health Records shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C. Section 17921 and implementing regulations.

F. Electronic Protected Health Information (ePHI) means individually identifiable health information transmitted by electronic media or maintained in electronic media, including but not limited to electronic media as set forth under 45 CFR section 160.103.

G. Individually Identifiable Health Information means health information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer or health care clearinghouse, and relates to the past, present or future physical or mental health or condition of an individual, the provision of

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

H. Privacy Rule shall mean the HIPAA Regulations that are found at 45 CFR Parts 160 and 164, subparts A and E.

I. Protected Health Information (PHI) means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or is transmitted or maintained in any other form or medium, as set forth under 45 CFR Section 160.103 and as defined under HIPAA.

J. Required by law, as set forth under 45 CFR Section 164.103, means a mandate contained in law that compels an entity to make a use or disclosure of PHI that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants, subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information, and a civil or an authorized investigative demand. It also includes Medicare conditions of participation with respect to health care providers participating in the program, and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

K. Secretary means the Secretary of the U.S. Department of Health and Human Services ("HHS") or the Secretary's designee.

L. Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of Department PHI, or confidential data utilized by Contractor to perform the services, functions and activities on behalf of Department as set forth in Section 1.A. of Exhibit E-1 of this Agreement; or interference with system operations in an information system that processes, maintains or stores Department PHI.

M. Security Rule shall mean the HIPAA regulations that are found at 45 CFR Parts 160 and 164.

N. Unsecured PHI shall have the meaning given to such term under the HITECH Act, 42 U.S.C. Section 17932(h), any guidance issued by the

Secretary pursuant to such Act and the HIPAA regulations.

3. Terms of Agreement.

A. **Permitted Uses and Disclosures of Department PHI by Contractor.**

Except as otherwise indicated in this Exhibit E-1, Contractor may use or disclose Department PHI only to perform functions, activities or services specified in Section 1.A of Exhibit E-1 of this Agreement, for, or on behalf of the Department, provided that such use or disclosure would not violate the HIPAA regulations or the limitations set forth in 42 CFR Part 2, or any other applicable law, if done by the Department. Any such use or disclosure, if not for purposes of treatment activities of a health care provider as defined by the Privacy Rule, must, to the extent practicable, be limited to the limited data set, as defined in 45 CFR Section 164.514(e)(2), or, if needed, to the minimum necessary to accomplish the intended purpose of such use or disclosure, in compliance with the HITECH Act and any guidance issued pursuant to such Act, and the HIPAA regulations.

B. **Specific Use and Disclosure Provisions**. Except as otherwise indicated in this Exhibit E-1, Contractor may:

1) **Use and Disclose for Management and Administration**. Use and disclose Department PHI for the proper management and administration of the Contractor's business, provided that such disclosures are required by law, or the Contractor obtains reasonable assurances from the person to whom the information is disclosed, in accordance with section D(7) of this Exhibit E-1, that it will remain confidential and will be used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Contractor of any instances of which it is aware that the confidentiality of the information has been breached.

2) **Provision of Data Aggregation Services**. Use Department PHI to provide data aggregation services to the Department to the extent requested by the Department and agreed to by Contractor. Data aggregation means the combining of PHI created or received by the Contractor, as the Business Associate, on behalf of the Department with PHI received by the Business Associate in its capacity as the Business Associate of another covered entity, to permit data analyses that relate to the health care operations of the Department

C. **Prohibited Uses and Disclosures**

1) Contractor shall not disclose Department PHI about an individual to a health plan for payment or health care operations purposes if the Department PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full and the individual requests such restriction, in accordance with 42 U.S.C. Section 17935(a) and 45 CFR Section 164.522(a).

2) Contractor shall not directly or indirectly receive remuneration in exchange for Department PHI.

D. **Responsibilities of Contractor**

Contractor agrees:

1) **Nondisclosure**. Not to use or disclose Department PHI other than as permitted or required by this Agreement or as required by law, including but not limited to 42 CFR Part 2.

2) **Compliance with the HIPAA Security Rule**. To implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Department PHI, including electronic PHI, that it creates, receives, maintains, uses or transmits on behalf of the Department, in compliance with 45 CFR Sections 164.308, 164.310 and 164.312, and to prevent use or disclosure of Department PHI other than as provided for by this Agreement. Contractor shall implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of 45 CFR Section 164, subpart C, in compliance with 45 CFR Section164.316. 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 the Contractor's operations and the nature and scope of its activities, and which incorporates the requirements of section 3, Security, below. Contractor will provide the Department with its current and updated policies upon request.

3) **Security**. Contractor shall take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:

   a. Complying with all of the data system security precautions

listed in Attachment A, Data Security Requirements;

b. Achieving and maintaining compliance with the HIPAA Security Rule (45 CFR Parts 160 and 164), as necessary in conducting operations on behalf of DHCS under this Agreement; and

c. Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III- Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies.

4) **Security Officer**. Contractor shall designate a Security Officer to oversee its data security program who shall be responsible for carrying out the requirements of this section and for communicating on security matters with the Department.

5) **Mitigation of Harmful Effects**. To mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of Department PHI by Contractor or its subcontractors in violation of the requirements of this Exhibit E.

6) **Reporting Unauthorized Use or Disclosure.** To report to Department any use or disclosure of Department PHI not provided for by this Exhibit E of which it becomes aware.

7) **Contractor's Agents and Subcontractors**.

a. To enter into written agreements with any agents, including subcontractors and vendors to whom Contractor provides Department PHI, that impose the same restrictions and conditions on such agents, subcontractors and vendors that apply to Contractor with respect to such Department PHI under this Exhibit E, and that require compliance with all applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations, including the requirement that any agents, subcontractors or vendors implement reasonable and appropriate administrative, physical, and technical safeguards to protect such PHI. As required by HIPAA, the HITECH Act and the HIPAA regulations, including 45 CFR Sections 164.308 and 164.314, Contractor shall incorporate, when applicable, the relevant provisions of this Exhibit E-1 into each subcontract or subaward to such

agents, subcontractors and vendors, including the requirement that any security incidents or breaches of unsecured PHI be reported to Contractor.

b. In accordance with 45 CFR Section 164.504(e)(1)(ii), upon Contractor's knowledge of a material breach or violation by its subcontractor of the agreement between Contractor and the subcontractor, Contractor shall:

i) Provide an opportunity for the subcontractor to cure the breach or end the violation and terminate the agreement if the subcontractor does not cure the breach or end the violation within the time specified by the Department; or

ii) Immediately terminate the agreement if the subcontractor has breached a material term of the agreement and cure is not possible.

8) **Availability of Information to the Department and Individuals to Provide Access and Information:**

a. To provide access as the Department may require, and in the time and manner designated by the Department (upon reasonable notice and during Contractor's normal business hours) to Department PHI in a Designated Record Set, to the Department (or, as directed by the Department), to an Individual, in accordance with 45 CFR Section 164.524. Designated Record Set means the group of records maintained for the Department health plan under this Agreement that includes medical, dental and billing records about individuals; enrollment, payment, claims adjudication, and case or medical management systems maintained for the Department health plan for which Contractor is providing services under this Agreement; or those records used to make decisions about individuals on behalf of the Department. Contractor shall use the forms and processes developed by the Department for this purpose and shall respond to requests for access to records transmitted by the Department within fifteen (15) calendar days of receipt of the request by producing the records or verifying that there are none.

b. If Contractor maintains an Electronic Health Record with

PHI, and an individual requests a copy of such information in an electronic format, Contractor shall provide such information in an electronic format to enable the Department to fulfill its obligations under the HITECH Act, including but not limited to, 42 U.S.C. Section 17935(e) and the HIPAA regulations.

9) **Amendment of Department PHI**. To make any amendment(s) to Department PHI that were requested by a patient and that the Department directs or agrees should be made to assure compliance with 45 CFR Section 164.526, in the time and manner designated by the Department, with the Contractor being given a minimum of twenty (20) days within which to make the amendment.

10) **Internal Practices**. To make Contractor's internal practices, books and records relating to the use and disclosure of Department PHI available to the Department or to the Secretary, for purposes of determining the Department's compliance with the HIPAA regulations. If any information needed for this purpose is in the exclusive possession of any other entity or person and the other entity or person fails or refuses to furnish the information to Contractor, Contractor shall provide written notification to the Department and shall set forth the efforts it made to obtain the information.

11) **Documentation of Disclosures**. To document and make available to the Department or (at the direction of the Department) to an individual such disclosures of Department PHI, and information related to such disclosures, necessary to respond to a proper request by the subject Individual for an accounting of disclosures of such PHI, in accordance with the HITECH Act and its implementing regulations, including but not limited to 45 CFR Section 164.528 and 42 U.S.C. Section 17935(c). If Contractor maintains electronic health records for the Department as of January 1, 2009 and later, Contractor must provide an accounting of disclosures, including those disclosures for treatment, payment or health care operations. The electronic accounting of disclosures shall be for disclosures during the three years prior to the request for an accounting.

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

a. **Initial Notice to the Department.** (1) To notify the Department **immediately by telephone call or email or fax** upon the discovery of a breach of unsecured PHI in electronic media or in any other media if the PHI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person. (2) To notify the Department **within 24 hours (one hour if SSA data) by email or fax** of the discovery of any suspected security incident, intrusion or unauthorized access, use or disclosure of PHI in violation of this Agreement or this Exhibit E-1, or potential loss of confidential data affecting this Agreement. A breach shall be treated as discovered by Contractor as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of Contractor.

Notice shall be provided to the Information Protection Unit, Office of HIPAA Compliance. If the incident occurs after business hours or on a weekend or holiday and involves electronic PHI, notice shall be provided by calling the Information Protection Unit (916.445.4646, 866-866-0602) or by emailing privacyofficer@dhcs.ca.gov). Notice shall be made using the DHCS "Privacy Incident Report" form, including all information known at the time. Contractor shall use the most current version of this form, which is posted on the DHCS Information Security Officer website (www.dhcs.ca.gov, then select "Privacy" in the left column and then "Business Partner" near the middle of the page) or use this link: http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/DHCSBusinessAssociatesOnly.aspx

Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of Department PHI, Contractor shall take:

i) Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and

ii) Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

b. **Investigation and Investigation Report.** To immediately investigate such suspected security incident, security incident, breach, or unauthorized access, use or disclosure of PHI . Within 72 hours of the discovery, Contractor shall submit an updated "Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the Information Protection Unit.

c. **Complete Report.** To provide a complete report of the investigation to the Department Program Contract Manager and the Information Protection Unit within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on the "Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable provisions of HIPAA, the HITECH Act, and the HIPAA regulations. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If the Department requests information in addition to that listed on the "Privacy Incident Report" form, Contractor shall make reasonable efforts to provide the Department with such information. If, because of the circumstances of the incident, Contractor needs more than ten (10) working days from the discovery to submit a complete report, the Department may grant a reasonable extension of time, in which case Contractor shall submit periodic updates until the complete report is submitted. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "Privacy Incident Report" form. The Department will review and approve the determination of whether a breach occurred and whether individual notifications and a corrective action plan are required.

d. **Responsibility for Reporting of Breaches.** If the cause of a breach of Department PHI is attributable to Contractor or its agents, subcontractors or vendors, Contractor is responsible for all required reporting of the breach as specified in 42 U.S.C. section 17932 and its implementing regulations,

including notification to media outlets and to the Secretary (after obtaining prior written approval of DHCS). If a breach of unsecured Department PHI involves more than 500 residents of the State of California or under its jurisdiction, Contractor shall first notify DHCS, then the Secretary of the breach immediately upon discovery of the breach. If a breach involves more than 500 California residents, Contractor shall also provide, after obtaining written prior approval of DHCS, notice to the Attorney General for the State of California, Privacy Enforcement Section. If Contractor has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to the Department in addition to Contractor, Contractor shall notify the Department, and the Department and Contractor may take appropriate action to prevent duplicate reporting.

e. **Responsibility for Notification of Affected Individuals.** If the cause of a breach of Department PHI is attributable to Contractor or its agents, subcontractors or vendors and notification of the affected individuals is required under state or federal law, Contractor shall bear all costs of such notifications as well as any costs associated with the breach. In addition, the Department reserves the right to require Contractor to notify such affected individuals, which notifications shall comply with the requirements set forth in 42U.S.C. section 17932 and its implementing regulations, including, but not limited to, the requirement that the notifications be made without unreasonable delay and in no event later than 60 calendar days after discovery of the breach. The Department Privacy Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made. The Department will provide its review and approval expeditiously and without unreasonable delay.

f. **Department Contact Information.** To direct communications to the above referenced Department staff, the Contractor shall initiate contact as indicated herein. The Department reserves the right to make changes to the contact information below by giving written notice to the Contractor. Said changes shall not require an amendment to this Addendum or the Agreement to which it is incorporated.

Department Program Contract Manager	DHCS Privacy Officer	DHCS Information Security Officer
See the Exhibit A, Scope of Work for Program Contract Manager information	Information Protection Unit c/o: Office of HIPAA Compliance Department of Health Care Services P.O. Box 997413, MS 4722 Sacramento, CA 95899-7413 (916) 445-4646; (866) 866-0602 Email: privacyofficer@dhcs.ca.gov Fax: (916) 440-7680	Information Security Officer DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95899-7413 Email: iso@dhcs.ca.gov Telephone: ITSD Service Desk (916) 440-7000; (800) 579-0874 Fax: (916)440-5537

13) **Termination of Agreement.** In accordance with Section 13404(b) of the HITECH Act and to the extent required by the HIPAA regulations, if Contractor knows of a material breach or violation by the Department of this Exhibit E-1, it shall take the following steps:

a. Provide an opportunity for the Department to cure the breach or end the violation and terminate the Agreement if the Department does not cure the breach or end the violation within the time specified by Contractor; or

b. Immediately terminate the Agreement if the Department has breached a material term of the Exhibit E-1 and cure is not possible.

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

E. Obligations of the Department.

The Department agrees to:

1) **Permission by Individuals for Use and Disclosure of PHI**. Provide the Contractor with any changes in, or revocation of, permission by an Individual to use or disclose Department PHI, if such changes affect the Contractor's permitted or required uses and disclosures.

2) **Notification of Restrictions**. Notify the Contractor of any restriction to the use or disclosure of Department PHI that the Department has agreed to in accordance with 45 CFR Section 164.522, to the extent that such restriction may affect the Contractor's use or disclosure of PHI.

3) **Requests Conflicting with HIPAA Rules**. Not request the Contractor to use or disclose Department PHI in any manner that would not be permissible under the HIPAA regulations if done by the Department.

4) **Notice of Privacy Practices**. Provide Contractor with the web link to the Notice of Privacy Practices that DHCS produces in accordance with 45 CFR Section 164.520, as well as any changes to such notice. Visit the DHCS website to view the most current Notice of Privacy Practices at: http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/NoticeofPrivacyPractices.aspx or the DHCS website at www.dhcs.ca.gov (select "Privacy in the right column and "Notice of Privacy Practices" on the right side of the page).

F. Audits, Inspection and Enforcement

If Contractor is the subject of an audit, compliance review, or complaint investigation by the Secretary or the Office for Civil Rights, U.S. Department of Health and Human Services, that is related to the performance of its obligations pursuant to this HIPAA Business Associate Exhibit E-1,Contractor shall immediately notify the Department. Upon request from the Department, Contractor shall provide the Department with a copy of any Department PHI that Contractor, as the Business Associate, provides to the Secretary or the Office of Civil Rights concurrently with providing such PHI to the Secretary. Contractor is responsible for any civil penalties assessed due to an audit or investigation of Contractor, in accordance with 42 U.S.C. Section 17934(c).

G. Termination.

1) **Term.** The Term of this Exhibit E-1 shall extend beyond the termination of the Agreement and shall terminate when all Department PHI is destroyed or returned to the Department, in accordance with 45 CFR Section 164.504(e)(2)(ii)(J).

2) **Termination for Cause**. In accordance with 45 CFR Section 164.504(e)(1)(iii), upon the Department's knowledge of a material breach or violation of this Exhibit E-1 by Contractor, the Department shall:

   a. Provide an opportunity for Contractor to cure the breach or end the violation and terminate this Agreement if Contractor does not cure the breach or end the violation within the time specified by the Department; or

   b. Immediately terminate this Agreement if Contractor has breached a material term of this Exhibit E-1 and cure is not possible.

THE REST OF THIS PAGE IS INTENTIONALLY BLANK

EXHIBIT E-2

Privacy and Security of Personal Information and Personally Identifiable Information Not Subject to HIPAA

1. Recitals.

A. In addition to the Privacy and Security Rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) the Department is subject to various other legal and contractual requirements with respect to the personal information (PI) and personally identifiable information (PII) it maintains. These include:

1) The California Information Practices Act of 1977 (California Civil Code §§1798 et seq.),

2) The Agreement between the Social Security Administration (SSA) and the Department, known as the Information Exchange Agreement (IEA), which incorporates the Computer Matching and Privacy Protection Act Agreement (CMPPA) between the SSA and the California Health and Human Services Agency. The IEA, including the CMPPA is attached to this Exhibit E as Attachment B and is hereby incorporated in this Agreement.

3) Title 42 Code of Federal Regulations, Chapter I, Subchapter A, Part 2.

B. The purpose of this Exhibit E-2 is to set forth Contractor's privacy and security obligations with respect to PI and PII that Contractor may create, receive, maintain, use, or disclose for or on behalf of Department pursuant to this Agreement. Specifically this Exhibit applies to PI and PII which is not Protected Health Information (PHI) as defined by HIPAA and therefore is not addressed in Exhibit E-1 of this Agreement, the HIPAA Business Associate Addendum; however, to the extent that data is both PHI or ePHI and PII, both Exhibit E-1 and this Exhibit E-2 shall apply.

C. The IEA Agreement referenced in A.2) above requires the Department to extend its substantive privacy and security terms to subcontractors who receive data provided to DHCS by the Social Security Administration. If Contractor receives data from DHCS that includes data provided to DHCS by the Social Security Administration, Contractor must comply with the following specific sections of the IEA Agreement: E. Security Procedures, F. Contractor/Agent Responsibilities, and G. Safeguarding and Reporting Responsibilities for Personally Identifiable Information ("PII"), and in Attachment 4 to the IEA, Electronic Information Exchange Security Requirements, Guidelines and Procedures for Federal, State and Local

Agencies Exchanging Electronic Information with the Social Security Administration. Contractor must also ensure that any agents, including a subcontractor, to whom it provides DHCS data that includes data provided by the Social Security Administration, agree to the same requirements for privacy and security safeguards for such confidential data that apply to Contractor with respect to such information.

D. The terms used in this Exhibit E-2, but not otherwise defined, shall have the same meanings as those terms have in the above referenced statute and Agreement. Any reference to statutory, regulatory, or contractual language shall be to such language as in effect or as amended.

2. Definitions.

A. "Breach" shall have the meaning given to such term under the IEA and CMPPA. It shall include a "PII loss" as that term is defined in the CMPPA.

B. "Breach of the security of the system" shall have the meaning given to such term under the California Information Practices Act, Civil Code section 1798.29(f).

C. "CMPPA Agreement" means the Computer Matching and Privacy Protection Act Agreement between the Social Security Administration and the California Health and Human Services Agency (CHHS).

D. "Department PI" shall mean Personal Information, as defined below, accessed in a database maintained by the Department, received by Contractor from the Department or acquired or created by Contractor in connection with performing the functions, activities and services specified in this Agreement on behalf of the Department.

E. "IEA" shall mean the Information Exchange Agreement currently in effect between the Social Security Administration (SSA) and the California Department of Health Care Services (DHCS).

F. "Notice-triggering Personal Information" shall mean the personal information identified in Civil Code section 1798.29 whose unauthorized access may trigger notification requirements under Civil Code section 1798.29. For purposes of this provision, identity shall include, but not be limited to, name, address, email address, identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print, a photograph or a biometric identifier. Notice-triggering Personal Information includes PI in electronic, paper or any other medium.

G. "Personally Identifiable Information" (PII) shall have the meaning given to such term in the IEA and CMPPA.

H. "Personal Information" (PI) shall have the meaning given to such term in California Civil Code Section 1798.3(a).

I. "Required by law" means a mandate contained in law that compels an entity to make a use or disclosure of PI or PII that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants, subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information, and a civil or an authorized investigative demand. It also includes Medicare conditions of participation with respect to health care providers participating in the program, and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

J. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PI, or confidential data utilized in complying with this Agreement; or interference with system operations in an information system that processes, maintains or stores PI.

3. Terms of Agreement

A. **Permitted Uses and Disclosures of Department PI and PII by Contractor**

Except as otherwise indicated in this Exhibit E-2, Contractor may use or disclose Department PI only to perform functions, activities or services for or on behalf of the Department pursuant to the terms of this Agreement provided that such use or disclosure would not violate the California Information Practices Act (CIPA) if done by the Department.

B. **Responsibilities of Contractor**

Contractor agrees:

1) **Nondisclosure.** Not to use or disclose Department PI or PII other than as permitted or required by this Agreement or as required by applicable state and federal law.

2) **Safeguards.** To implement appropriate and reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of Department PI and PII, to protect against anticipated threats or hazards to the security or integrity of Department PI and PII, and to prevent use or disclosure of Department PI or PII other than as provided for by this Agreement. Contractor shall develop and maintain a written information privacy and security program that include administrative, technical and physical safeguards appropriate to the size and complexity of Contractor's operations and the nature and scope of its activities, which incorporate the requirements of section 3, Security, below. Contractor will provide DHCS with its current policies upon request.

3) **Security.** Contractor shall take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI and/or PI, and to protect paper documents containing PHI and/or PI. These steps shall include, at a minimum:

a. Complying with all of the data system security precautions listed in Attachment A, Business Associate Data Security Requirements;

b. Providing a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III- Security of Federal Automated Information Systems, which sets forth guidelines for automated information systems in Federal agencies; and

c. If the data obtained by Contractor from DHCS includes PII, Contractor shall also comply with the substantive privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement between the SSA and the California Health and Human Services Agency (CHHS) and in the Agreement between the SSA and DHCS, known as the Information Exchange Agreement, which are attached as Attachment B and incorporated into this Agreement. The specific sections of the IEA with substantive privacy and security requirements to be complied with are sections E, F, and G, and in Attachment 4 to the IEA, Electronic Information Exchange Security Requirements, Guidelines and Procedures for Federal, State and Local Agencies Exchanging Electronic Information with the SSA. Contractor also agrees to ensure that any agents, including a subcontractor to whom it provides

DHCS PII, agree to the same requirements for privacy and security safeguards for confidential data that apply to Contractor with respect to such information.

4) **Mitigation of Harmful Effects.** To mitigate, to the extent practicable, any harmful effect that is known to Contractor of a use or disclosure of Department PI or PII by Contractor or its subcontractors in violation of this Exhibit E-2.

5) **Contractor's Agents and Subcontractors.** To impose the same restrictions and conditions set forth in this Exhibit E-2 on any subcontractors or other agents with whom Contractor subcontracts any activities under this Agreement that involve the disclosure of Department PI or PII to the subcontractor.

6) **Availability of Information to DHCS.** To make Department PI and PII available to the Department for purposes of oversight, inspection, amendment, and response to requests for records, injunctions, judgments, and orders for production of Department PI and PII. If Contractor receives Department PII, upon request by DHCS, Contractor shall provide DHCS with a list of all employees, contractors and agents who have access to Department PII, including employees, contractors and agents of its subcontractors and agents.

7) **Cooperation with DHCS.** With respect to Department PI, to cooperate with and assist the Department to the extent necessary to ensure the Department's compliance with the applicable terms of the CIPA including, but not limited to, accounting of disclosures of Department PI, correction of errors in Department PI, production of Department PI, disclosure of a security breach involving Department PI and notice of such breach to the affected individual(s).

8) **Confidentiality of Alcohol and Drug Abuse Patient Records.** Contractor agrees to comply with all confidentiality requirements set forth in Title 42 Code of Federal Regulations, Chapter I, Subchapter A, Part 2. Contractor is aware that criminal penalties may be imposed for a violation of these confidentiality requirements.

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

   a. Initial Notice to the Department. (1) To notify the Department

immediately by telephone call or email or fax upon the discovery of a breach of unsecured Department PI or PII in electronic media or in any other media if the PI or PII was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, or upon discovery of a suspected security incident involving Department PII. (2) To notify the Department **within one (1) hour by email or fax** if the data is data subject to the SSA Agreement; and **within 24 hours by email or fax** of the discovery of any suspected security incident, intrusion or unauthorized access, use or disclosure of Department PI or PII in violation of this Agreement or this Exhibit E-1 or potential loss of confidential data affecting this Agreement. A breach shall be treated as discovered by Contractor as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of Contractor.

b. Notice shall be provided to the Information Protection Unit, Office of HIPAA Compliance. If the incident occurs after business hours or on a weekend or holiday and involves electronic Department PI or PII, notice shall be provided by calling the Department Information Security Officer. Notice shall be made using the DHCS "Privacy Incident Report" form, including all information known at the time. Contractor shall use the most current version of this form, which is posted on the DHCS Information Security Officer website (www.dhcs.ca.gov, then select "Privacy" in the left column and then "Business Partner" near the middle of the page) or use this link: http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/DHCSBusinessAssociatesOnly.aspx .

c. Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of Department PI or PII, Contractor shall take:

i. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and

ii. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and

regulations.

d. **Investigation and Investigation Report**. To immediately investigate such suspected security incident, security incident, breach, or unauthorized access, use or disclosure of PHI. Within 72 hours of the discovery, Contractor shall submit an updated "Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the Department Information Security Officer.

e. **Complete Report**. To provide a complete report of the investigation to the Department Program Contract Manager and the Information Protection Unit within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. The report shall be submitted on the "Privacy Incident Report" form and shall include an assessment of all known factors relevant to a determination of whether a breach occurred. The report shall also include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If the Department requests information in addition to that listed on the "Privacy Incident Report" form, Contractor shall make reasonable efforts to provide the Department with such information. If, because of the circumstances of the incident, Contractor needs more than ten (10) working days from the discovery to submit a complete report, the Department may grant a reasonable extension of time, in which case Contractor shall submit periodic updates until the complete report is submitted. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "Privacy Incident Report" form. The Department will review and approve the determination of whether a breach occurred and whether individual notifications and a corrective action plan are required.

f. **Responsibility for Reporting of Breaches.** If the cause of a breach of Department PI or PII is attributable to Contractor or its agents, subcontractors or vendors, Contractor is responsible for all required reporting of the breach as specified in CIPA, section 1798.29and as may be required under the IEA. Contractor shall bear all costs of required

notifications to individuals as well as any costs associated with the breach. The Privacy Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made. The Department will provide its review and approval expeditiously and without unreasonable delay.

g. If Contractor has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to the Department in addition to Contractor, Contractor shall notify the Department, and the Department and Contractor may take appropriate action to prevent duplicate reporting.

h. **Department Contact Information**. To direct communications to the above referenced Department staff, the Contractor shall initiate contact as indicated herein. The Department reserves the right to make changes to the contact information below by giving written notice to the Contractor. Said changes shall not require an amendment to this Addendum or the Agreement to which it is incorporated.

Department Program Contract	**DHCS Privacy Officer**	**DHCS Information Security Officer**
See the Exhibit A, Scope of Work for Program Contract Manager information	Information Protection Unit c/o: Office of HIPAA Compliance Department of Health Care Services P.O. Box 997413, MS 4722 Sacramento, CA 95899-7413 (916) 445-4646 Email: privacyofficer@dhcs.ca.gov Telephone:(916) 445-4646	Information Security Officer DHCS Information Security Office P.O. Box 997413, MS 6400 Sacramento, CA 95899-7413 Email: iso@dhcs.ca.gov Telephone: ITSD Service Desk (916) 440-7000 or (800) 579-0874

10) Designation of Individual Responsible for Security

Contractor shall designate an individual, (e.g., Security Officer), to oversee its data security program who shall be responsible for carrying out the requirements of this Exhibit E-2 and for communicating on security matters with the Department.

EXHIBIT E-3

Miscellaneous Terms and Conditions

Applicable to Exhibit E

1) **Disclaimer**. The Department makes no warranty or representation that compliance by Contractor with this Exhibit E, HIPAA or the HIPAA regulations will be adequate or satisfactory for Contractor's own purposes or that any information in Contractor's possession or control, or transmitted or received by Contractor, is or will be secure from unauthorized use or disclosure. Contractor is solely responsible for all decisions made by Contractor regarding the safeguarding of the Department PHI, PI and PII.

2) **Amendment**. The parties acknowledge that federal and state laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Exhibit E may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, and the HIPAA regulations, and other applicable state and federal laws. Upon either party's request, the other party agrees to promptly enter into negotiations concerning an amendment to this Exhibit E embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, and the HIPAA regulations, and other applicable state and federal laws. The Department may terminate this Agreement upon thirty (30) days written notice in the event:

   a) Contractor does not promptly enter into negotiations to amend this Exhibit E when requested by the Department pursuant to this section; or

   b) Contractor does not enter into an amendment providing assurances regarding the safeguarding of Department PHI that the Department deems is necessary to satisfy the standards and requirements of HIPAA and the HIPAA regulations.

3) **Judicial or Administrative Proceedings**. Contractor will notify the Department if it is named as a defendant in a criminal proceeding for a violation of HIPAA or other security or privacy law. The Department may terminate this Agreement if Contractor is found guilty of a criminal violation of HIPAA. The Department may terminate this Agreement if a finding or stipulation that the Contractor has violated any standard or requirement of HIPAA, or other security or privacy laws is made in any administrative or civil proceeding in which the Contractor is a party or

has been joined. DHCS will consider the nature and seriousness of the violation in deciding whether or not to terminate the Agreement.

4) **Assistance in Litigation or Administrative Proceedings.** Contractor shall make itself and any subcontractors, employees or agents assisting Contractor in the performance of its obligations under this Agreement, available to the Department at no cost to the Department to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against the Department, its directors, officers or employees based upon claimed violation of HIPAA, or the HIPAA regulations, which involves inactions or actions by the Contractor, except where Contractor or its subcontractor, employee or agent is a named adverse party.

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

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

7) **Conflict.** In case of a conflict between any applicable privacy or security rules, laws, regulations or standards the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to PHI, PI and PII from unauthorized disclosure. Further, Contractor must comply within a reasonable period of time with changes to these standards that occur after the effective date of this Agreement.

8) **Regulatory References.** A reference in the terms and conditions of this Exhibit E to a section in the HIPAA regulations means the section as in effect or as amended.

9) **Survival.** The respective rights and obligations of Contractor under Section 3, Item D of Exhibit E-1, and Section 3, Item B of Exhibit E-2, Responsibilities of Contractor, shall survive the termination or expiration of this Agreement.

10) **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.

11) **Audits, Inspection and Enforcement.** From time to time, and subject to all applicable federal and state privacy and security laws and regulations, the Department may conduct a reasonable inspection of the facilities, systems, books and records of Contractor to monitor compliance with this Exhibit E. Contractor shall promptly remedy any violation of any provision of this Exhibit E. The fact that the Department 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 Exhibit E. The Department's failure to detect a non-compliant practice, or a failure to report a detected non-compliant practice to Contractor does not constitute acceptance of such practice or a waiver of the Department's enforcement rights under this Agreement, including this Exhibit E.

12) **Due Diligence.** Contractor shall exercise due diligence and shall take reasonable steps to ensure that it remains in compliance with this Exhibit E and is in compliance with applicable provisions of HIPAA, the HITECH Act and the HIPAA regulations, and other applicable state and federal law, and that its agents, subcontractors and vendors are in compliance with their obligations as required by this Exhibit E.

13) **Term.** The Term of this Exhibit E-1 shall extend beyond the termination of the Agreement and shall terminate when all Department PHI is destroyed or returned to the Department, in accordance with 45 CFR Section 164.504(e)(2)(ii)(I), and when all Department PI and PII is destroyed in accordance with Attachment A.

14) **Effect of Termination**. Upon termination or expiration of this Agreement for any reason, Contractor shall return or destroy all Department PHI, PI and PII that Contractor still maintains in any form, and shall retain no copies of such PHI, PI or PII. If return or destruction is not feasible, Contractor shall notify the Department of the conditions that make the return or destruction infeasible, and the Department and Contractor shall determine the terms and conditions under which Contractor may retain the PHI, PI or PII. Contractor shall continue to extend the protections of this Exhibit E to such Department PHI, PI and PII, and shall limit further use of such data to those purposes that make the return or destruction of such data infeasible. This provision shall apply to Department PHI, PI and PII that is in the possession of subcontractors or agents of Contractor.

Attachment A
Data Security Requirements

1. Personnel Controls

A. **Employee Training**. All workforce members who assist in the performance of functions or activities on behalf of the Department, or access or disclose Department PHI or 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 six (6) years following termination of this Agreement.

B. **Employee Discipline**. Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.

C. **Confidentiality Statement**. All persons that will be working with Department PHI or PI must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to Department PHI or PI. The statement must be renewed annually. The Contractor shall retain each person's written confidentiality statement for Department inspection for a period of six (6) years following termination of this Agreement.

D. **Background Check**. Before a member of the workforce may access Department 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 three (3) years.

2. Technical Security Controls

A. **Workstation/Laptop encryption**. All workstations and laptops that store Department 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 by the Department Information Security Office.

B. **Server Security**. Servers containing unencrypted Department PHI or PI must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

C. **Minimum Necessary**. Only the minimum necessary amount of Department PHI or PI required to perform necessary business functions may be copied, downloaded, or exported.

D. **Removable media devices**. All electronic files that contain Department PHI or PI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, Blackberry, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.

E. **Antivirus software**. All workstations, laptops and other systems that process and/or store Department PHI or PI must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

F. **Patch Management**. All workstations, laptops and other systems that process and/or store Department PHI or PI must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within 30 days of vendor release. 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. Applications and systems that cannot be patched must have compensatory controls implemented to minimize risk, where possible.

G. **User IDs and Password Controls**. All users must be issued a unique user name for accessing Department 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 90 days, preferably every 60 days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:

1) Upper case letters (A-Z)
2) Lower case letters (a-z)
3) Arabic numerals (0-9)
4) Non-alphanumeric characters (punctuation symbols)

H. **Data Destruction**. When no longer needed, all Department PHI or PI must be wiped using the Gutmann or US Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission of the Department Information Security Office.

I. **System Timeout**. The system providing access to Department PHI or PI must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.

J. **Warning Banners**. All systems providing access to Department PHI or PI must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.

K. **System Logging**. The system must maintain an automated audit trail which can identify the user or system process which initiates a request for Department PHI or PI, or which alters Department 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 Department PHI or PI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.

L. **Access Controls**. The system providing access to Department PHI or PI must use role based access controls for all user authentications, enforcing the principle of least privilege.

M. **Transmission encryption**. All data transmissions of Department 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 Department PHI can be encrypted. This requirement pertains to any type of Department PHI or PI in motion such as website access, file transfer, and E-Mail.

N. **Intrusion Detection**. All systems involved in accessing, holding, transporting, and protecting Department PHI or PI that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

3. Audit Controls

A. **System Security Review**. Contractor must ensure audit control mechanisms that record and examine system activity are in place. All systems processing and/or storing Department PHI or PI must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools.

B. **Log Reviews**. All systems processing and/or storing Department PHI or PI must have a routine procedure in place to review system logs for unauthorized access.

C. **Change Control**. All systems processing and/or storing Department PHI or PI must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity and availability of data.

4. Business Continuity / Disaster Recovery Controls

A. **Emergency Mode Operation Plan.** Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of Department 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.

B. **Data Backup Plan**. Contractor must have established documented procedures to backup Department PHI to maintain retrievable exact copies of Department 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 Department PHI or PI should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of Department data.

5. Paper Document Controls

A. **Supervision of Data**. Department 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. Department PHI or PI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

B. **Escorting Visitors**. Visitors to areas where Department PHI or PI is contained shall be escorted and Department PHI or PI shall be kept out of sight while visitors are in the area.

C. **Confidential Destruction**. Department PHI or PI must be disposed of through confidential means, such as cross cut shredding and pulverizing.

D. **Removal of Data**. Only the minimum necessary Department PHI or PI may be removed from the premises of the Contractor except with express written permission of the Department. Department 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 Contractors locations.

E. **Faxing**. Faxes containing Department PHI or PI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.

F. **Mailing**. Mailings containing Department 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 Department 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 the Department to use another method is obtained.