DEPARTMENT OF MENTAL HEALTH

recovery. wellbeing.

JONATHAN E. SHERIN, M.D., Ph.D.
Director

Gregory C. Polk, M.P.A.
Chief Deputy Director

Curley L. Bonds, M.D.
Chief Medical Officer

Lisa H. Wong, Psy.D.
Senior Deputy Director

December 1, 2020

APPROVED BY THE CEO
DEC 01 2020
BY DELEGATED AUTHORITY

The Honorable Board of Supervisors
County of Los Angeles
383 Kenneth Hahn Hall of Administration
500 West Temple Street
Los Angeles, CA 90012

Dear Supervisors:

APPROVAL TO EXTEND THE TERM OF 29 EXISTING FEE-FOR-SERVICE MEDI-CAL ACUTE PSYCHIATRIC INPATIENT HOSPITAL SERVICE AGREEMENTS AND TWO SOLE SOURCE INDIGENT ACUTE PSYCHIATRIC INPATIENT HOSPITAL SERVICE AGREEMENTS
(ALL SUPERVISORIAL DISTRICTS)
(3 VOTES)

SUBJECT

Request approval to extend the term of 29 existing Fee-for-Service Medi-Cal Acute Psychiatric Inpatient Hospital Service Agreements and two sole source Indigent Acute Psychiatric Inpatient Hospital Service Agreements. The extensions will ensure that medically necessary acute psychiatric inpatient hospital services are continuously provided for Medi-Cal beneficiaries and for the uninsured clients residing in Los Angeles County while the Department of Mental Health and the State of California, Department of Health Care Services develop performance measures for new contracts.

IT IS RECOMMENDED THAT YOUR BOARD:

1. Approve and authorize the Department of Mental Health (DMH) Director, or his designee, to prepare, sign, and execute amendments substantially similar to Attachment I to extend the term of the 29 existing Fee-for-Service Medi-Cal Acute Psychiatric Inpatient Hospital (FFS Hospital) Service Agreements listed on Attachment II for the continued provision of medically necessary acute psychiatric inpatient hospital services for Medi-Cal beneficiaries. The amendments will be

effective January 1, 2021, through June 30, 2021, with an option to extend the term for one additional fiscal year, as necessary. These contracts do not have a maximum contract amount as reimbursement for acute psychiatric inpatient hospital services will be on a fee-for-service basis. The total aggregate estimated cost of the extension for six months is $69,415,923, fully funded by 2011 Realignment, 2011 Realignment-Managed Care, 2011 Realignment-Early and Periodic Screening Diagnosis and Treatment (EPSDT), and Federal Financial Participation (FFP) Medi-Cal revenues.

2. Approve and authorize the Director, or his designee, to prepare, sign, and execute amendments substantially similar to Attachment III to extend the term of two sole source Indigent Acute Psychiatric Inpatient Hospital (Indigent Hospital) Service Agreements with Aurora Charter Oak-Los Angeles, LLC (Aurora Charter Oak), and College Hospital-Cerritos (College Hospital) for the continued provision of acute psychiatric inpatient hospital services for uninsured clients. The extension amendments for Aurora Charter Oak and College Hospital will be effective January 1, 2021, through June 30, 2021, with an option to extend the term for one additional fiscal year, as necessary. For the six-month extension period, the Maximum Contract Amount (MCA) is $1,388,117 for Aurora Charter Oak and $927,465 for College Hospital, fully funded by 2011 Realignment revenue.

3. Delegate authority to the Director, or his designee, to prepare, sign, and execute future FFS Hospital Service Agreements with appropriately licensed hospitals, as necessary, provided that: 1) sufficient funds are available; 2) County Counsel approves the agreement as to form; and 3) the Director, or his designee, provides written notification to the Board and the Chief Executive Officer (CEO).

4. Delegate authority to the Director, or his designee, to prepare, sign, and execute future amendments to the FFS Hospital Service Agreements and Indigent Hospital Service Agreements described in Recommendations 1, 2, and 3 to increase the contract rates; add, delete, modify or replace the Statements of Work/Service Exhibits; and/or reflect federal, State, and/or County regulatory and/or policy changes provided that sufficient funds are available; and the amendments will be subject to prior review and approval as to form by County Counsel, with written notice to the Board and CEO.

5. Delegate authority to the Director, or his designee, to terminate the Agreements described in Recommendations 1, 2, and 3 in accordance with the termination provisions of the Agreements, including Termination for Convenience. The Director, or his designee, will notify the Board and CEO, in writing, of such termination action.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

Board approval of the first Recommendation will authorize the Director, or his designee, to extend the term of 29 FFS Hospital Service Agreements for the continued provision of acute psychiatric inpatient hospital services for Medi-Cal beneficiaries, effective January 1, 2021, through June 30, 2021, with an option to extend the term for one additional fiscal year.

Board approval of the second Recommendation will enable DMH to execute an amendment to extend the term of the sole source Indigent Hospital Service Agreements with Aurora Charter Oak and College Hospital, effective January 1, 2021, through June 30, 2021, with an option to extend the term for one additional fiscal year. The extensions will allow DMH to provide continuous acute psychiatric inpatient hospital services for uninsured clients.

Board approval of the third Recommendation will allow DMH to execute future FFS Service Agreements with other licensed hospitals as necessary.

Board approval of the fourth Recommendation will allow DMH to amend the FFS Hospital Service Agreements and Indigent Hospital Service Agreements described in Recommendations 1, 2, and 3 to add, delete, modify, or replace the Statements of Work/Service Exhibits; reflect federal, State, and/or County regulatory and/or policy changes; and modify the contract rates, provided that sufficient funds are available and the amendments will be subject to prior review and approval as to form by County Counsel, with written notice to the Board and CEO.

Board approval of the fifth Recommendation will allow DMH to terminate the Agreements described in Recommendation 1, 2, and 3 in accordance with the contract's termination provisions, including Termination for Convenience, in a timely manner, as necessary.

Implementation of Strategic Plan Goals

The recommended actions are consistent with the County's Strategic Plan Goal I, Make Investments that Transform Lives, specifically Strategy I.2 – Enhance Our Delivery of Comprehensive Interventions.

FISCAL IMPACT/FINANCING

The estimated cost for these actions is $71,731,505, fully funded by 2011 Realignment, 2011 Realignment–Managed Care, 2011 Realignment–EPSDT and FFP Medi-Cal revenues. The funding for these contracts are included in DMH's FY 2020-21 Adopted budget.

There is no net County cost associated with the recommended actions.

FACTS AND PROVISIONS/LEGAL REQUIREMENTS

The current FFS Hospital Service Agreements and two sole source Indigent Hospital Service Agreements listed on Attachment II expire on December 31, 2020. DMH requires Board approval to extend the term of these contracts while DMH develops new performance measures for new Acute Psychiatric Inpatient Hospital Contracts, which requires collaboration with the State of California, Department of Health Care Services (DHCS) and contractors. DMH will return to your Board to execute new Acute Psychiatric Inpatient Hospital Contracts upon completion. Board approval is required to extend these existing Agreements to ensure that continuous medically necessary acute psychiatric inpatient hospital services are provided to Medi-Cal beneficiaries and to the uninsured clients residing in Los Angeles County (County).

Through the Mental Health Plan (MHP) Agreement between the State DHCS and the County, DMH operates as the local MHP responsible for the provision of specialty mental health services under Welfare and Institutions Code (WIC) Section 14712. Under the MHP Agreement, DMH is responsible for administering all Medi-Cal specialty mental health services to care for eligible Medi-Cal beneficiaries residing in the County in accordance with Title 9, California Code of Regulations (CCR) and to ensure that comprehensive quality services are provided to severely mentally ill clients residing in the County.

Each of the hospitals listed on Attachment II are qualified Lanterman-Petris-Short (LPS) designated hospitals to detain, evaluate, and provide treatment to clients pursuant to WIC Section 5150. These hospitals will provide continuous twenty-four hours per day, seven days per week (24/7) intensive psychiatric services in a licensed Acute Psychiatric Hospital or a distinct acute psychiatric part of a licensed General Acute Care Hospital, with the specific intent to ameliorate the symptoms of danger to self or others, or the inability to provide for food, clothing, and shelter due to a mental disability as determined by a qualified mental health professional staff of the facility.

As mandated by your Board, the performance of all contractors is evaluated by DMH on an annual basis to ensure the contractor's compliance with all contract terms and performance standards.

Attachment I is the extension amendment for DMH's existing 29 FFS Hospitals. Attachment II lists the FFS Hospitals and their addresses, as well as the Service Area SA), and Supervisorial District(s) served. Attachment III is the extension amendment for the two sole source Indigent Hospital Service Agreements with Aurora Charter Oak and College Hospital.

Under Board Policy No. 5.100 (Sole Source Contracts), DMH is required to provide your Board advance notification for amendments to existing contracts when departments do not have delegated authority to extend the term of the current contract. DMH is requesting an exemption to the Board's Sole Source Contracts policy for the purposes of the FFS Hospital Agreements, because DMH is required as the MHP to ensure that comprehensive quality services are provided to severely mentally ill clients residing in the County. In addition, as the MHP, DMH has an open application process for licensed hospitals to apply for a FFS Hospital Agreement if they meet County requirements.

DMH notified your Board of its intent to extend the terms of Aurora Charter Oak and College Hospital's sole source Indigent Hospital Service Agreements on October 22, 2020 (Attachment IV). The extension of these sole source Indigent Hospital Service Agreements will ensure continuous acute psychiatric inpatient hospital services for uninsured clients while DMH and the State DHCS develop new performance measures for the new contracts. Aurora Charter Oak and College Hospital are located in SAs 3 and 7, which were identified as strategic SAs in the County's Psychiatric Emergency Services Relief Plan approved by your Board in July 2005 to address overcrowding at County hospitals. The required Sole Source Checklist (Attachment V), identifying and justifying the need for these sole source extensions, has been approved by the CEO.

IMPACT ON CURRENT SERVICES (OR PROJECTS)

These recommended actions will allow DMH to provide continuous medically necessary acute psychiatric inpatient hospital services for Medi-Cal beneficiaries and uninsured clients residing in the County.

Respectfully submitted,

JONATHAN E. SHERIN, M.D., Ph.D.
Director

JES:GCP:ES
SK:sc

Attachments

c: Executive Office, Board of Supervisors
Chief Executive Office
County Counsel
Chairperson, Mental Health Commission

CONTRACT NO. MH0600XX

AMENDMENT NO. __

THIS AMENDMENT is made and entered into this ____ day of January, 2021, by and between the COUNTY OF LOS ANGELES (hereafter "County"), and _____ (hereafter "Contractor").

WHEREAS, reference is made to that certain document entitled "Mental Health Services Agreement Contract Allowable Rate Fee-For-Service Medi-Cal Acute Psychiatric Inpatient Hospital Services", dated July 1, 2015, and further identified as County Agreement No. MH0600XX, and any amendments thereto (hereafter collectively "Agreement"); and

WHEREAS, on June 2, 2015, the County Board of Supervisors delegated authority to the Director of Mental Health, or designee, to execute amendments to the Agreement that include authority to modify the Agreement language to reflect federal, State, and County regulatory and/or policy changes, and make other designated changes; and

WHEREAS, on December 1, 2020, the County Board of Supervisors delegated authority to the Director of Mental Health, or designee, to execute amendments to the Agreement that include authority to extend the term of the Agreement and modify the Agreement language to reflect federal, State, and/or County regulatory and/or policy changes, and make other designated changes; and

WHEREAS, said Agreement provides that changes may be made in the form of a written amendment which is formally approved and executed by the parties; and

WHEREAS, for Fiscal Year (FY) 2020-21, County and Contractor intend to amend the Agreement to extend the term of the Agreement for the six-month period beginning January 1, 2021 through June 30, 2021, and update certain other terms and conditions; and

WHEREAS, Contractor warrants that it continues to possess the competence, expertise, and personnel necessary to provide services consistent with the requirements of the Agreement, and consistent with the professional standard of care for these services.

NOW, THEREFORE, County and Contractor agree that the Agreement shall be amended only as follows:

1. This amendment is effective upon execution.
2. The term of the Agreement is extended for six months, for the period of January 1, 2021 through June 30, 2021.
3. Attachment X shall be deleted in its entirety, and replaced with "Attachment X-__," attached hereto and incorporated herein by reference. All references to Attachment X shall be deemed amended to state "Attachment X-__".
4. Attachment XII-__ (BUSINESS ASSOCIATE AGREEMENT UNDER THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)), attached hereto and incorporated herein by reference, shall be added to the Agreement.
5. Attachment XIII-__ (DMH BUSINESS ASSOCIATE/CONTRACTOR'S COMPLIANCE WITH INFORMATION SECURITY REQUIREMENTS EXHIBIT), attached hereto and incorporated herein by reference, shall be added to the Agreement.

6. Attachment XIV-___ (INFORMATION SECURITY CONTRACT/AGREEMENT REQUIREMENTS), attached hereto and incorporated herein by reference, shall be added to the Agreement.
7. Contractor shall provide services in accordance with Contractor's FY_____ Contract Package for this Agreement and any addenda thereto approved in writing by County's Director of Mental Health or his designee.
8. Except as provided in this Amendment, all other terms and conditions of the Agreement shall remain in full force and effect.

/

/

/

/

/

/

/

/

/

/

/

/

/

/

/

IN WITNESS WHEREOF, the Board of Supervisors of the County of Los Angeles has caused this Amendment to be subscribed by the County's Director of Mental Health or his designee, and Contractor has caused this Amendment to be subscribed on its behalf by its duly authorized officer, on the day, month, and year first above written.

COUNTY OF LOS ANGELES

By_____
Jonathan E. Sherin, M.D., Ph.D.
Director of Mental Health

_____
CONTRACTOR

By _____

Name_____

Title _____
(AFFIX CORPORATE SEAL HERE)

APPROVED AS TO FORM:
OFFICE OF THE COUNTY COUNSEL

By: Emily D. Issa
Deputy County Counsel

LOS ANGELES COUNTY
DEPARTMENT OF MENTAL HEALTH
hope. recovery. wellbeing.

CHIEF INFORMATION OFFICE BUREAU

ELECTRONIC DATA TRANSMISSION TRADING PARTNER AGREEMENT (TPA)

This Trading Partner Agreement ('Agreement') is made and entered by and between the Legal Entity or Network Provider named _____ ("Trading Partner"), whose legal entity or Network Provider number is _____ and the County of Los Angeles – Department of Mental Health ("DMH").

WHEREAS, DMH and Trading Partner exchange information and data electronically in connection with certain healthcare transactions; and

WHEREAS, DMH and Trading Partner will be readily equipped at their own expense with the Systems and trained personnel necessary to engage in the successful exchange of electronic information and data; and

WHEREAS, in the electronic transmission of information and data, the confidentiality and security of the data which is exchanged between the Parties is of the highest priority to both Parties; and

WHEREAS, it is anticipated by DMH that the Trading Partner may use, in the performance of this Agreement, various third parties as the Trading Partner's Agents in the electronic exchange of information;

NOW THEREFORE, in consideration for the mutual promises herein, the Parties agree as follows:

1. DEFINITIONS

1.1. Agents
Third parties or organizations that contract with the Trading Partner to perform designated services in order to facilitate the electronic transfer of data. Examples of Agents include claims clearinghouses, vendors, and billing services.

1.2. Confidential Information
Information relating to specific Individuals which is exchanged by and between DMH, the Trading Partner, and/or the Agents for various business purposes, but which is protected from disclosure to unauthorized persons or entities by The Privacy Act of 1974, The Administrative Simplification Provisions of the federal Health Insurance Portability and Accountability Act and regulations promulgated there under ("HIPAA"). The Insurance Information and Privacy Protections Act, or other applicable state and federal statutes and regulations, which shall hereinafter be collectively referred to as "Privacy Statutes and Regulations."

1.3. Covered Individuals
Individual persons who are eligible for payment of certain services or prescriptions rendered or sold to them under the terms, conditions, limitations and exclusions of a health benefit program administered by DMH or by some other Payor.

1.4. Data
A formalized representation of specific facts or concepts suitable for communication, interpretation, or processing by people or by automatic means.

1.5. Data Log
A complete written summary of Data and Data Transmissions exchanged between the Parties over the period of time this Agreement is in effect and, including, without limitation, sender and receiver information, the date and time of transmission and the general nature of the transmission.

1.6. Data Transmission
The automated transfer or exchange of data between Trading Partners or their agents, by means of their systems which are compatible for that purpose, pursuant to the terms and conditions set forth in this Agreement.

1.7. Data Universal Numbering System ("DUNS")
Data Universal Numbering System (DUNS) – A unique nine-digit identification number assigned by Dun & Bradstreet (D&B) to a Trading Partner or Agent for the purpose of identifying a business entity. The DUNS can be requested at: http://fedgov.dnb.com/webform.

1.8. Digital Key Certificate
Software that resides on Trading Partner's workstation or server assigned to the Trading Partner by DMH for the purpose of successfully executing Data Transmissions or otherwise carrying out the express terms of this Agreement.

1.9. Electronic Data Interchange ("EDI")
The automated exchange of business data from application to application in an ANSI approved or other mutually agreed format.

1.10. Electronic Remittance Advice ("ERA")
A transaction containing information pertaining to the disposition of a specific claim field with DMH by Providers for payment of services rendered to an Individual.

1.11. Envelope
A control structure in a mutually agreed format for the electronic interchange of one or more encoded Data Transmissions either sent or received by the Parties to this Agreement.

1.12. Individual
An individual person(s) whose claims for payment of services may be eligible to be paid, under the terms of the applicable federal, state or local governmental program for which DMH processes or administers claims. It is acknowledged and agreed between the Parties that claim payments for purposes of this Agreement will be made directly to Providers on behalf of such Individuals.

1.13. Lost or Indecipherable Transmission
A Data Transmission which is never received by or cannot be processed to completion by the receiving Party in the format or composition received because it is garbled or incomplete, regardless of how or why the message was rendered garbled or incomplete.

1.14. Payee National Provider Identifier ("NPI")
The National Provider Identifier that is specific to the Legal Entity, FFS Group, or FFS Organization. Solo practitioners will enter their individual NPI number in this field.

1.15. Payor
A business organization that provides benefit payments on behalf of Covered Individuals eligible for payment for certain services to Covered Individuals.

1.16. Provider
Hospitals, clinics or persons duly licensed or certified to provide mental health services to Covered Individuals of Los Angeles County.

1.17. Secure Identification Cards
Those cards assigned to the Trading Partner or Agent by DMH for allowing the Trading Partner to transfer files electronically to DMH.

1.18. Source Documents
Documents containing Data which is or may be required as part of Data Transmission with respect to a claim for payment for mental health services rendered to an eligible Individual. Examples of Data contained within a specific Source Document include, without limitation, the following: Individual's name and identification number, claim number, diagnosis code for the service rendered, dates of service, procedure code, applicable charges, the Provider's name and/or provider number.

1.19. Submitter ID Number
A unique number assigned by DMH to the Trading Partner or Agent for the purpose of identifying the Trading Partner for Data Transmissions.

1.20. System
The equipment and software necessary for a successful electronic Data Transmission.

1.21. Trading Partner
A Provider who has entered into this Agreement with DMH in order to satisfy all or part of its obligations under a Legal Entity Agreement or Network Provider Agreement by means of EDI.

2. TERM AND TERMINATION

2.1. Term of Agreement
This Agreement will be effective on the day the Trading Partner Agreement is approved by the Department of Mental Health and shall continue in full force until terminated by either party.

2.2. Voluntary Termination
Either Party may terminate this Agreement for its own convenience on thirty (30) days advance written notice to the other Party.

2.3. Termination for Cause
Either party may terminate this Agreement upon ten (10) working days advance written notice to the other Party upon the default by the other Party of any material obligation hereunder, which default is incapable of cure or which, being capable of cure, has not been cured within 30 days after receipt of written notice with reasonable specificity of such default (or such additional cure period as the non-defaulting Party may authorize). However, in the event of a breach by the Trading Partner of the terms of Article IV, Section 4.3 (Express Warranties Regarding Agents) or any Section of Article V (CONFIDENTIALITY AND SECURITY), or in the event a change of ownership of the Trading Partner or its Agents as defined by Article VII Section 7.12 (Change in Ownership of Trading Partner or its Agents) takes place, DMH shall have the unilateral right to

terminate this Agreement immediately without prior notice to the Trading Partner. However, in its right to exercise immediate termination, DMH shall provide the Trading Partner with written notice the day the termination occurs.

3. OBLIGATIONS OF THE PARTIES

3.1. Mutual Obligations

In addition to the obligations of the respective Parties which are set forth elsewhere in this Agreement, the mutual obligations of DMH, the Trading Partner and/or the Trading Partner's Agents collectively referred to as "the Parties" shall include, but not be limited to, the following:

(a) Accuracy of EDI Transmission

The Parties shall take reasonable care to ensure that Data and Data Transmissions are timely, complete, accurate and secure, and shall take reasonable precautions to prevent unauthorized access to the System of the other Party, the Data Transmission itself or the contents of an Envelope which is transmitted either to or from either Party pursuant to this Agreement.

(b) Re-transmission of Indecipherable Transmissions

Where there is evidence that a Data Transmission is Lost or Indecipherable Transmission, the sending Party shall make best efforts to trace and re-transmit the original Data Transmission in a manner which allows it to be processed by the receiving Party as soon as practicable.

(c) Cost of Equipment

Each Party shall, at its own expense, obtain and maintain its own System and shall update its System as recommended by the manufacturer/owner/licensor of said System. Furthermore, each Party shall pay its own costs for any and all charges related to Data Transmission under this Agreement and specifically including, without limitation, charges for System equipment, software and services, charges for maintaining an electronic mailbox, connect time, terminals, connections, telephones, modems, and any applicable minimum use charges. Each Party shall also be responsible for any and all expenses it incurs for translating, formatting, or sending and receiving communications over the electronic network to the electronic mailbox, if any, of the other Party.

(d) Back-up Files

Each Party shall maintain adequate back-up files and/or electronic tapes or other means sufficient to re-create a Data Transmission in the event that such re-creation becomes necessary for any purpose at any time. Such back-up files and/or tapes shall be subject to the terms of this Agreement to the same extent as the original Data Transmission.

(e) Format of Transmissions

Except as otherwise provided herein, each Party shall send and receive all Data Transmissions in the ANSI approved format, or such other format as DMH shall designate in writing to the Trading Partner.

(f) Testing

Each Party shall, prior to the initial Data Transmission and throughout the term of this Agreement, test and cooperate with the other Party in the testing of the Systems of both Parties as DMH considers reasonably necessary to ensure the accuracy, timeliness, completeness and confidentiality of each Data Transmission.

3.2. Trading Partner Obligations

In addition to the requirements of Section 3.1 and 5.1 and this section (3.2), the Trading Partner shall also be specifically obligated as follows:

(a) To refrain from copying, reverse engineering, disclosing, publishing, distributing or altering any Data, Data Transmissions or the contents of an Envelope, except as necessary to comply with the terms of this Agreement, or use the same for any purpose other than that for which the Trading Partner was specifically given access and authorization by DMH;

(b) To refrain from obtaining by any means to any Data, Data Transmission, Envelope or DMH's System for any purpose other than that which the Trading Partner has received express authorization to receive access. Furthermore, in the event that the Trading Partner receives Data or Data Transmissions, which are clearly not intended for the receipt of the Trading Partner, the Trading Partner shall immediately notify DMH and make arrangements to return the Data or Data Transmission or re-transmit the Data or Data Transmission to DMH. After such re-transmission, the Trading Partner shall immediately delete the Data contained in such Data Transmission from its System.

(c) To install necessary security precautions to ensure the security of the System or records relating to the System of both DMH and the Trading Partner when the System is not in active use by the Trading Partner.

(d) To protect and maintain at all times the confidentiality of Secure Identification Cards issued by DMH to the Trading Partner or Agent.

(e) To provide special protection for security and other purposes where appropriate, by means of authentication, encryption, the use of passwords or by other mutually agreed means, to those specific Data Transmissions which the Parties agree should be so protected shall use at least the same level of protection for any subsequent transmission of the original Data Transmission.

(f) Prior to or upon execution of this Agreement, to provide DMH in writing with all of the information requested in the Trading Partner Information section of the Trading Partner Agreement (TPA) online application. While this Agreement is in effect, the Trading Partner shall notify DMH in writing within five (5) business days of any material changes in the information originally provided by the Trading Partner in the TPA online application.

(e) To minimize Data Transmission loss, Trading Partners must notify DMH when System changes are planned by the Trading Partner at least thirty (30) days prior to the change taking place.

3.3. DMH Obligations

In addition to the obligations of DMH which are set forth herein, DMH shall also be specifically obligated as follows:

(a) Availability of Data

DMH shall subject to the terms of this Agreement, make available to the Trading Partner by electronic means those types of Data and Data Transmissions to which the Trading Partner is entitled to receive by mutual agreement of the Parties or as provided by law.

(b) Notices Regarding Formats

DMH shall provide Trading Partners a written listing of acceptable electronic data transmission formats (e.g., PDF, XLS, Doc). Should the need arise for DMH to make changes to these transmission formats, the trading Partner will receive no less than 14 days written notice.

4. AGENTS

4.1. Responsibility for Agents

If the Trading Partner uses the services of an Agent in any capacity in order to receive, transmit, store or otherwise process Data or Data Transmissions or perform related activities, the Trading Partner shall be fully liable to DMH or for any acts, failures or omissions of the Agent in providing said services as though they were the Trading Partner's own acts, failures, or missions.

4.2. Notices Regarding Agents

Prior to the commencement of the Agent's services in the performance of this Agreement, the Trading Partner shall designate, in the TPA online application, its specific Agents who are authorized to send and/or receive Data Transmissions in the performance of this Agreement on behalf of the Trading Partner. Except as provided otherwise in the Agreement, the Trading Partner shall notify DMH of any material changes in the information contained in the TPA online application, no less than 14 days prior to the effective date of such changes. The information within the TPA application, when fully executed shall be incorporated into this Agreement by reference and shall be effective on the date of its execution, unless specified otherwise. The Trading Partner's designation of its Agent for purposes of this Agreement is expressly subject to the approval of DMH, which approval shall not be unreasonably withheld.

4.3. Express Warranties Regarding Agents

The Trading Partner expressly warrants that the Agent will make no changes in the Data content of any and all Data Transmissions or the contents of an Envelope, and further that such Agent will take all appropriate measures to maintain the timeliness, accuracy, confidentiality and completeness of each 'Data Transmission. Furthermore, the Trading Partner expressly warrants that its Agents will be specifically advised of, and will comply in all respects with, the terms of this Agreement.

4.4. Indemnification Regarding Agents

The Trading Partner shall indemnify, defend and hold harmless DMH from any and all claims, actions, damages, liabilities, costs and expenses, specifically including, without limitation, reasonable attorney's fees and costs resulting from the acts or omissions of the Trading Partner, its Agents, employees, subcontractors in the performance of this Agreement; provided however, that DMH shall have the option, at its sole discretion, to employ attorneys selected by it to defend any such action, the costs and expenses of which shall be the responsibility of the Trading Partner. DMH for its part shall provide the Trading Partner with timely notice of the existence of such proceedings and such information, documents and other cooperation as reasonably necessary to assist the Trading Partner in establishing a defense to such action. These indemnities shall survive termination of this Agreement and DMH reserves the right, at its option and expense, to participate in the defense of any suit or proceeding through counsel of its own choosing.

5. CONFIDENTIALITY AND SECURITY

5.1 General Requirements

In addition to the requirements of Section 3.1 and 3.2, the Trading Partner shall maintain adequate security procedures to prevent unauthorized access to Data, Data Transmissions, or the System of DMH, and shall immediately notify DMH of any and all unauthorized attempts by any person or entity to obtain access to or otherwise tamper with the Data, Data Transmissions or the System of DMH.

(a) Confidential Information

The Trading Partner further agrees to hold DMH harmless for any and all claims or causes of action brought by any party, including third parties, arising from any unauthorized disclosure of Confidential Information by or on behalf of the Trading Partner. In addition, the Trading Partner shall in its performance under this Agreement, comply with any and all applicable Privacy Statutes and Regulations (as defined in Article I, Section 1.4 (Confidential Information) relating to Confidential Information and agrees to maintain the confidentiality of such Confidential Information for the benefit of such Individuals or of DMH as is required by such Privacy Statutes and Regulations. Such Confidential Information concerning Individuals includes, but is not limited to, medical records and information regarding claims and payment of the claims of Individuals.

(b) Notice of Unauthorized Disclosures

The Trading Partner will promptly notify DMH of any and all unlawful or unauthorized disclosures of Confidential Information that comes to its attention and will cooperate with DMH in the event any litigation arises concerning the unauthorized use, transfer or disclosure of Confidential Information.

6. RECORDS RETENTION AND AUDIT

6.1 Records Retention

The Trading Partner shall maintain, for a period of no less than seven (7) years from the date of its receipt complete, (except for children for whom records should be retained until 18 years of age) or until the audit is settled, accurate and unaltered copies of any and all Source Documents from all Data Transmissions.

6.2 Electronic Transmission and Audit Logs

Both Parties shall establish and maintain Logs which shall record any and all Data Transmissions taking place between the Parties during the term of this Agreement. Each Party will take necessary and reasonable steps to ensure that all Logs constitutes a current, accurate, complete and unaltered record of any and all Data Transmissions between the Parties, and shall be retained by each Party for no less than twenty-four (24) months following the date of the Data Transmission. The Log may be maintained on computer media or other suitable means provided that, if it is necessary to do so, the information contained in the Log may be timely retrieved and presented in readable form.

7. MISCELLANEOUS

7.1 Amendments

This Agreement may not be changed or modified in any manner except by an instrument in writing signed by a duly authorized officer of each of the Parties hereto.

7.2 Dispute Resolution

With the exception of disputes which are the subject of immediate termination as set forth in this Agreement, the Parties hereby agree that, in the event of a dispute or alleged breach of the terms of this Agreement between the Parties, they will work together in good faith first, to resolve the matter internally and within a reasonable period of time by escalating it as reasonably necessary to higher levels of management of each of the respective Parties, and, then if necessary, to use a mutually agreed alternative dispute resolution technique prior to resorting to litigation, with the exception of disputes involving either fraud or breaches of the

requirements of section 5 (CONFIDENTIALITY AND SECURITY), in which case either Party shall be free to seek available remedies in any appropriate forum at any time.

7.3 Mutual Compliance with Applicable Laws and Regulations
The Parties hereby mutually agree that they will, in the performance of the terms of this Agreement, comply in all respects with any and all applicable local, state and federal ordinances, statutes, regulations, or orders of courts of competent jurisdiction.

7.4 Force Majeure
Each Party shall be excused from performance for any period of time during this Agreement to the extent that it is prevented from performing any obligation of service, in whole or in part, as a result of causes beyond the reasonable control and without the fault or negligence of such Party. Such acts include without limitation, strikes, lockouts, riots, acts of war, fire, communication line failures, power failures, earthquakes, floods or natural disasters. Delays in performance due to the occurrence of such events shall automatically extend such dates for a period equal to the duration of such events. However, such automatic extension shall have no effect on the exercise of either Party's right of voluntary termination as set forth in Section 2.2 (Term of Agreement).

7.5 Change of Ownership of Trading Partner
The Trading Partner shall notify DMH no less than ten days in advance of any transfer of ownership interest in the Trading Partner's business or any transfer of ownership in the business of the Trading Partner's Agent. Furthermore, notwithstanding the providing of notice regarding changes in the ownership of the Trading Partner as required by this section, no such changes in ownership or other information provided by the Trading Partner will alter in any way the obligations of the Parties under the terms of this Agreement without prior written agreement of DMH.

7.6 Notices
Any notices pertaining to this Agreement shall be given in writing and shall be deemed duly given when personally delivered to the Trading Partner or the Trading Partner's authorized representative.

COUNTY OF LOS ANGELES - DEPARTMENT OF MENTAL HEALTH

CHIEF INFORMATION OFFICE BUREAU

ELECTRONIC TRADING PARTNER AGREEMENT

By execution hereof by duly authorized representatives of both Parties, the Parties hereby acknowledge, agree to and shall be bound by all the terms, provisions and conditions of the Trading Partner Agreement.

Agreed To:

Trading Partner Name (Legal Entity / Network Provider)
(Type or Print)

Authorized Personnel (Type or Print)	**Authorized Signature**
Title (Type or Print)	**Date**

Agreed To:

COUNTY OF LOS ANGELES
DEPARTMENT OF MENTAL HEALTH
695 S. VERMONT AVE., LOS ANGELES CA 90005

Please complete form, print, scan and attach to TPA request for processing.

LOS ANGELES COUNTY
DEPARTMENT OF MENTAL HEALTH
hope. recovery. wellbeing.

COUNTY OF LOS ANGELES
DEPARTMENT OF MENTAL HEALTH
CHIEF INFORMATION OFFICE BUREAU

CONFIDENTIALITY OATH

Non-LACDMH Workforce Members

(Note: Authorized signatory must sign at time of contract execution. For employee(s) and non-employee(s), Contractor shall make available within three (3) business days upon DMH request)

ANNUAL

The intent of this Confidentiality Form is to ensure that all Business Associates, Contractors, Consultants, Interns, Volunteers, Locum Tenens, Non-Governmental Agencies (NGA), Fee-For-Service Hospitals (FFS1), Fee-For-Service Outpatient (FFS2) and Pharmacy users are aware of their responsibilities and accountability to protect the confidentiality of clients' sensitive information viewed, maintained and/or accessed by any DMH on-line systems.

Further, the Department's Medi-Cal and MEDS access policy has been established in accordance with federal and state laws governing confidentiality.

The California Welfare and Institutions Code (WIC) Section 14100.2, cites the information to be regarded confidential. This information includes applicant/beneficiary names, addresses, services provided, social and economic conditions or circumstances, agency evaluation of personal information, and medical data. (See also 22 California Code of Regulations (C.C.R.), Sections 50111 and 51009)

The Medi-Cal Eligibility Manual, Section 2-H, titled "Confidentiality of Medi-Cal Case Records," referring to WIC Section 14100.2, a, b, f, and h, provides in part that:

"(a) All types of information, whether written or oral, concerning a person, made or kept by any public office or agency in connection with the administration of any provision of this chapter *… shall be confidential, and shall not be open to examination other than for purposes directly connected with administration of the Medi-Cal program."

"(b) Except as provided in this section and to the extent permitted by Federal Law or regulation, all information about applicants and recipients as provided for in subdivision (a) to be safeguarded includes, but is not limited to, names and addresses, medical services provided, social and economic conditions or circumstances, agency evaluation or personal information, and medical data, including diagnosis and past history of disease or disability."

"(f) The State Department of Health Services may make rules and regulations governing the custody, use and preservation of all records, papers, files, and communications pertaining to the administration of the laws relating to the Medi-Cal program **…."

"(h) Any person who knowingly releases or possesses confidential information concerning persons who have applied for or who have been granted any form of Medi-Cal benefits ***… for which State or Federal funds are made available in violation of this section is guilty of a misdemeanor."

***, **, *** The State of California's Statute for Medicaid Confidentiality can be found at the following web address: http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/Medicaidstatute.aspx**

Please read the agreement and take due time to consider it prior to signing.

I understand that Contractors, Consultants, Interns, Volunteers, Locum Tenens, Non-Governmental Agencies (NGA), Fee-For-Service Hospitals (FFS1), Fee-For-Service Outpatient (FFS2) and Pharmacy users are prohibited from sharing their unique logon I.D. and password with anyone.

Further, I understand that data browsing is strictly prohibited and my access to information is restricted to the minimum necessary required to carry out my job responsibilities.

Further, I understand that obtaining, releasing, or using confidential client information from case records or computer records for purposes not specifically related to the administration of services and authorized by WIC Section 14100.2 is prohibited.

Further, I understand the violation of the confidentiality of records or of these policies which are made for protection of the confidentiality of such records, may cause:

1. A civil action under the following provisions of WIC section 5330:
   a) Any person may bring an action against an individual who has willfully and knowingly released confidential information or records concerning him or her in violation of this chapter, or of Chapter 1 (commencing with Section 11860) of Part 3 of Division 10.5 of the Health and Safety Code, for the greater of the following amounts:
      1. Ten thousand Dollars ($10,000).
      2. Three times the amount of actual damages, if any sustained by the plaintiff.
   b) Any person may bring an action against an individual who has negligently released confidential information or records concerning him or her in violation of this chapter, or of Chapter 1 (commencing with Section 11860) of Part 3 of Division 10.5 of the Health and Safety Code, for both of the following:
      1. One thousand dollars ($1,000) in order to recover under this paragraph; it shall not be a prerequisite that the plaintiff suffer or be threatened with actual damages.
      2. The amount of actual damages, if any, sustained by the plaintiff.
   c) Any person may, in accordance with Chapter 3 (commencing with Section 525) of Title 7 of Part 2 of the Code of Civil Procedure, bring an action to enjoin the release of confidential information or records in violation of this chapter, and may in the same action seek damages as provided in this section.
   d) In addition to the amounts specified in subdivisions (a) and (b), the plaintiff shall recover court costs and reasonable attorney's fees as determined by the court.

2. Disciplinary action including suspension or termination of Contract.

3. Further, I understand that the County will not provide legal protection if violations of these policies or procedures occur.

I hereby certify that I have read this form and I hereby certify that I have read this form and I have knowledge of the requirements of State and Federal confidentiality laws and will comply with all applicable provisions of same.

I, the undersigned, hereby agree not to divulge any information or records concerning any client except in accordance with WIC Section 5328 et seq. and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). I acknowledge that the unauthorized release of confidential information as described in this document may result in disciplinary action up to and including termination of any County Contract or removal of my ability to provide work under a County Contract. I further agree I have read as described in this document that a person may make me subject to a civil action under the provisions of the W&I Code for the unauthorized release of confidential information.

User's Name: _____ / _____ / _____
Print **Signature** **Date**

Provider Name: _____ **/ Provider #:** _____ **/ Phone #: ( ) _____**

Address: _____ / _____ / _____ / _____
City **Zip Code** **Service Area**

The signed copy of this agreement must be maintained by Business Associate / Contractor

LOS ANGELES COUNTY
DEPARTMENT OF
MENTAL HEALTH
hope. recovery. wellbeing.

ELECTRONIC SIGNATURE AGREEMENT
Non-LACDMH User

This Agreement governs the rights, duties, and responsibilities of Department of Mental Health in the use of an electronic signature in County of Los Angeles. In addition, I, the undersigned, understand that this Agreement describes my obligations to protect my electronic signature, and to notify appropriate authorities if it is stolen, lost, compromised, unaccounted for, or destroyed.

I agree to the following terms and conditions:

I agree that my electronic signature will be valid upon the date of issuance until it is revoked or terminated per the terms of this agreement. I agree that I will be required annually to renew my electronic signature and I will be notified and given the opportunity to renew my electronic signature each year and shall do so. The terms of this Agreement shall apply to each such renewal unless superseded.

I will use my electronic signature to establish my identity and sign electronic documents and forms. I am solely responsible for protecting my electronic signature. If I suspect or discover that my electronic signature has been stolen, lost, used by an unauthorized party, or otherwise compromised, then I will immediately notify DMH Helpdesk and request that my electronic signature be revoked. I will then immediately cease all use of my electronic signature. I agree to keep my electronic signature secret and secure by taking reasonable security measures to prevent it from being lost, modified or otherwise compromised, and to prevent unauthorized disclosure of, access to, or use of it or of any media on which information about it is stored.

I will immediately request that my electronic signature be revoked if I discover or suspect that it has been or is in danger of being lost, disclosed, compromised or subjected to unauthorized use in any way. I understand that I may also request revocation at any time for any other reason.

If I have requested that my electronic signature be revoked, or I am notified that someone has requested that my electronic signature be suspended or revoked, and I suspect or discover that it has been or may be compromised or subjected to unauthorized use in any way, I will immediately cease using my electronic signature. I will also immediately cease using my electronic signature upon termination of employment or termination of this Agreement.

I further agree that, for the purposes of authorizing and authenticating electronic health records, my electronic signature has the full force and effect of a signature affixed by hand to a paper document.

Additionally, I am responsible for ensuring that all employees, contractors, volunteers, interns, trainees, or persons whose conduct in the performance of work for LACDMH is under my authority, regardless of whether are paid or unpaid by the County, which are authorized to access Sensitive Information or Confidential Data through LACDMH Systems, have received and signed this Electronic Signature Agreement.

Business Associate / Contractor Workforce Member's Name	Business Associate / Contractor Workforce Member's Signature	Date

As a representative and Liaison of the Business Associate / Contractor performing in a management or supervisory capacity, I certify that the above signer, whose conduct in the performance of work for accessing LACDMH resources is under my authority, has acknowledged and signed this agreement.

Business Associate / Contractor Manager's Name	Business Associate / Contractor Manager's Signature	Date

LOS ANGELES COUNTY
DEPARTMENT OF
MENTAL HEALTH
hope. recovery. wellbeing.

BUSINESS ASSOCIATE AGREEMENT UNDER THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

County is a Covered Entity as defined by, and subject to the requirements and prohibitions of, the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA), and regulations promulgated thereunder, including the Privacy, Security, Breach Notification, and Enforcement Rules at 45 Code of Federal Regulations (C.F.R.) Parts 160 and 164 (collectively, the "HIPAA Rules").

Contractor performs or provides functions, activities or services to County that require Contractor in order to provide such functions, activities or services to create, access, receive, maintain, and/or transmit information that includes or that may include Protected Health Information, as defined by the HIPAA Rules. As such, Contractor is a Business Associate, as defined by the HIPAA Rules, and is therefore subject to those provisions of the HIPAA Rules that are applicable to Business Associates.

The HIPAA Rules require a written agreement ("Business Associate Agreement") between County and Contractor in order to mandate certain protections for the privacy and security of Protected Health Information, and these HIPAA Rules prohibit the disclosure to or use of Protected Health Information by Contractor if such an agreement is not in place.

This Business Associate Agreement and its provisions are intended to protect the privacy and provide for the security of Protected Health Information disclosed to or used by Contractor in compliance with the HIPAA Rules.

Therefore, the parties agree as follows:

1. DEFINITIONS

1.1 "Breach" has the same meaning as the term "breach" at 45 C.F.R. § 164.402.

1.2 "Business Associate" has the same meaning as the term "business associate" at 45 C.F.R. § 160.103. For the convenience of the parties, a "business associate" is a person or entity, other than a member of the workforce of covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to Protected Health Information. A "business associate" also is a subcontractor that creates, receives, maintains, or transmits Protected Health Information on behalf of another business associate. And in

reference to the party to this Business Associate Agreement "Business Associate" shall mean Contractor.

1.3 "Covered Entity" has the same meaning as the term “covered entity” at 45 C.F.R. § 160.103, and in reference to the party to this Business Associate Agreement, "Covered Entity" shall mean County.

1.4 "Data Aggregation" has the same meaning as the term "data aggregation" at 45 C.F.R. § 164.501.

1.5 "De-identification" refers to the de-identification standard at 45 C.F.R. § 164.514.

1.6 "Designated Record Set" has the same meaning as the term "designated record set" at 45 C.F.R. § 164.501.

1.7 "Disclose” and “Disclosure” mean, with respect to Protected Health Information, the release, transfer, provision of access to, or divulging in any other manner of Protected Health Information outside Business Associate’s internal operations or to other than its workforce. (See 45 C.F.R. § 160.103.)

1.8 "Electronic Health Record” means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff. (See 42 U.S. C. § 17921.)

1.9 “Electronic Media” has the same meaning as the term “electronic media” at 45 C.F.R. § 160.103. For the convenience of the parties, electronic media means (1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

1.10 "Electronic Protected Health Information” has the same meaning as the term “electronic protected health information” at 45 C.F.R. § 160.103, limited to Protected Health Information created or received by Business Associate from or on behalf of Covered

Entity. For the convenience of the parties, Electronic Protected Health Information means Protected Health Information that is (i) transmitted by electronic media; (ii) maintained in electronic media.

1.11 "Health Care Operations" has the same meaning as the term "health care operations" at 45 C.F.R. § 164.501.

1.12 "Individual" has the same meaning as the term "individual" at 45 C.F.R. § 160.103. For the convenience of the parties, Individual means the person who is the subject of Protected Health Information and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502 (g).

1.13 "Law Enforcement Official" has the same meaning as the term "law enforcement official" at 45 C.F.R. § 164.103.

1.14 "Minimum Necessary" refers to the minimum necessary standard at 45 C.F.R. § 164.502 (b).

1.15 "Protected Health Information" has the same meaning as the term "protected health information" at 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity. For the convenience of the parties, Protected Health Information includes information that (i) 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; (ii) identifies the Individual (or for which there is a reasonable basis for believing that the information can be used to identify the Individual); and (iii) is created, received, maintained, or transmitted by Business Associate from or on behalf of Covered Entity, and includes Protected Health Information that is made accessible to Business Associate by Covered Entity. "Protected Health Information" includes Electronic Protected Health Information.

1.16 "Required by Law" has the same meaning as the term "required by law" at 45 C.F.R. § 164.103.

1.17 "Secretary" has the same meaning as the term "secretary" at 45 C.F.R. § 160.103

1.18 "Security Incident" has the same meaning as the term "security incident" at 45 C.F.R. § 164.304.

1.19 "Services" means, unless otherwise specified, those functions, activities, or services in the applicable underlying Agreement, Contract, Master Agreement, Work Order, or Purchase Order or

other service arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

1.20 "Subcontractor" has the same meaning as the term "subcontractor" at 45 C.F.R. § 160.103.

1.21 "Unsecured Protected Health Information" has the same meaning as the term “unsecured protected health information" at 45 C.F.R. § 164.402.

1.22 “Use” or “Uses” means, with respect to Protected Health Information, the sharing, employment, application, utilization, examination or analysis of such Information within Business Associate’s internal operations. (See 45 C.F.R § 164.103.)

1.23 Terms used, but not otherwise defined in this Business Associate Agreement, have the same meaning as those terms in the HIPAA Rules.

2. PERMITTED AND REQUIRED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

2.1 Business Associate may only Use and/or Disclose Protected Health Information as necessary to perform Services, and/or as necessary to comply with the obligations of this Business Associate Agreement.

2.2 Business Associate may Use Protected Health Information for de-identification of the information if de-identification of the information is required to provide Services.

2.3 Business Associate may Use or Disclose Protected Health Information as Required by Law.

2.4 Business Associate shall make Uses and Disclosures and requests for Protected Health Information consistent with the Covered Entity’s applicable Minimum Necessary policies and procedures.

2.5 Business Associate may Use Protected Health Information as necessary for the proper management and administration of its business or to carry out its legal responsibilities.

2.6 Business Associate may Disclose Protected Health Information as necessary for the proper management and administration of its business or to carry out its legal responsibilities, provided the Disclosure is Required by Law or Business Associate obtains reasonable assurances from the person to whom the Protected Health Information is disclosed (i.e., the recipient) that it will be held confidentially and Used or further Disclosed only as Required by

Law or for the purposes for which it was disclosed to the recipient and the recipient notifies Business Associate of any instances of which it is aware in which the confidentiality of the Protected Health Information has been breached.

2.7 Business Associate may provide Data Aggregation services relating to Covered Entity's Health Care Operations if such Data Aggregation services are necessary in order to provide Services.

3. PROHIBITED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

3.1 Business Associate shall not Use or Disclose Protected Health Information other than as permitted or required by this Business Associate Agreement or as Required by Law.

3.2 Business Associate shall not Use or Disclose Protected Health Information in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by Covered Entity, except for the specific Uses and Disclosures set forth in Sections 2.5 and 2.6.

3.3 Business Associate shall not Use or Disclose Protected Health Information for de-identification of the information except as set forth in section 2.2.

4. OBLIGATIONS TO SAFEGUARD PROTECTED HEALTH INFORMATION

4.1 Business Associate shall implement, use, and maintain appropriate safeguards to prevent the Use or Disclosure of Protected Health Information other than as provided for by this Business Associate Agreement.

4.2 Business Associate shall comply with Subpart C of 45 C.F.R Part 164 with respect to Electronic Protected Health Information, to prevent the Use or Disclosure of such information other than as provided for by this Business Associate Agreement.

4.3 Business Associate shall be responsible for the provision of an annual mandatory information security and privacy training, for all staff that create, receive, maintain, or transmit Protected Health Information on behalf of Business Associate or the County, at the time of initial employment and on an ongoing basis as required by federal and State law, including but not limited to Health Insurance Portability and Accountability Act (HIPAA).

4.3.1 Business Associate shall monitor, track, document and make available upon request by the federal, State and/or County government the annual information security and privacy training (e.g., training bulletins/flyers, sign-in sheets

specifying name and function of staff, and/or individual certificates of completion, etc.) provided to Business Associate's workforce members, including clerical, administrative/management, clinical, subcontractors, and independent contractors that create, receive, maintain, or transmit Protected Health Information on behalf of Business Associate or the County.

4.4 Business Associate shall ensure that all workforce members, including clerical, administrative, management, clinical, subcontractors, and independent contractors that create, receive, maintain, or transmit Protected Health Information on behalf of Business Associate or the County, 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 sensitive content such as Protected Health Information. The statement must be renewed annually.

4.5 Appropriate sanctions must be applied against workforce members who fail to comply with any provisions of Business Associate's security and privacy policies and procedures, including termination of employment where appropriate.

5. <u>REPORTING NON-PERMITTED USES OR DISCLOSURES, SECURITY INCIDENTS, AND BREACHES OF UNSECURED PROTECTED HEALTH INFORMATION</u>

5.1 Business Associate shall report to Covered Entity any Use or Disclosure of Protected Health Information not permitted by this Business Associate Agreement, any Security Incident, and/ or any Breach of Unsecured Protected Health Information as further described in Sections 5.1.1, 5.1.2, and 5.1.3.

5.1.1 Business Associate shall report to Covered Entity any Use or Disclosure of Protected Health Information by Business Associate, its employees, representatives, agents or Subcontractors not provided for by this Agreement of which Business Associate becomes aware.

5.1.2 Business Associate shall report to Covered Entity any Security Incident of which Business Associate becomes aware.

5.1.3. Business Associate shall report to Covered Entity any Breach by Business Associate, its employees, representatives, agents, workforce members, or Subcontractors of Unsecured Protected Health Information that is known to Business Associate or, by exercising

reasonable diligence, would have been known to Business Associate. Business Associate shall be deemed to have knowledge of a Breach of Unsecured Protected Health Information if 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 Business Associate, including a Subcontractor, as determined in accordance with the federal common law of agency.

5.2 Except as provided in Section 5.3, for any reporting required by Section 5.1, Business Associate shall provide, to the extent available, all information required by, and within the times frames specified in, Sections 5.2.1 and 5.2.2.

5.2.1 Business Associate shall make an immediate telephonic report upon discovery of the non-permitted Use or Disclosure of Protected Health Information, Security Incident or Breach of Unsecured Protected Health Information to **(562) 940-3335** that minimally includes:

(a) A brief description of what happened, including the date of the non-permitted Use or Disclosure, Security Incident, or Breach and the date of Discovery of the non-permitted Use or Disclosure, Security Incident, or Breach, if known;

(b) The number of Individuals whose Protected Health Information is involved;

(c) A description of the specific type of Protected Health Information involved in the non-permitted Use or Disclosure, Security Incident, or Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved);

(d) The name and contact information for a person highly knowledge of the facts and circumstances of the non-permitted Use or Disclosure of PHI, Security Incident, or Breach

5.2.2 Business Associate shall make a <u>written report without unreasonable delay and in no event later than three (3) business days</u> from the date of discovery by Business Associate of the non-permitted Use or Disclosure of Protected Health Information, Security Incident, or Breach of Unsecured Protected Health Information and to the **HIPAA**

Compliance Officer at: Hall of Records, County of Los Angeles, Chief Executive Office, Risk Management Branch-Office of Privacy, 320 W. Temple Street, 7th Floor, Los Angeles, California 90012, PRIVACY@ceo.lacounty.gov, that includes, to the extent possible:

(a) A brief description of what happened, including the date of the non-permitted Use or Disclosure, Security Incident, or Breach and the date of Discovery of the non-permitted Use or Disclosure, Security Incident, or Breach, if known;

(b) The number of Individuals whose Protected Health Information is involved;

(c) A description of the specific type of Protected Health Information involved in the non-permitted Use or Disclosure, Security Incident, or Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved);

(d) The identification of each Individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been, accessed, acquired, Used, or Disclosed;

(e) Any other information necessary to conduct an assessment of whether notification to the Individual(s) under 45 C.F.R. § 164.404 is required;

(f) Any steps Business Associate believes that the Individual(s) could take to protect him or herself from potential harm from the non-permitted Use or Disclosure, Security Incident, or Breach;

(g) A brief description of what Business Associate is doing to investigate, to mitigate harm to the Individual(s), and to protect against any further similar occurrences; and

(h) The name and contact information for a person highly knowledge of the facts and circumstances of the non-permitted Use or Disclosure of PHI, Security Incident, or Breach.

5.2.3 If Business Associate is not able to provide the information specified in Section 5.2.1 or 5.2.2 at the time of the required report, Business Associate shall provide such information promptly thereafter as such information becomes available.

5.3 Business Associate may delay the notification required by Section 5.1.3, if a law enforcement official states to Business Associate that notification would impede a criminal investigation or cause damage to national security.

5.3.1 If the law enforcement official's statement is in writing and specifies the time for which a delay is required, Business Associate shall delay its reporting and/or notification obligation(s) for the time period specified by the official.

5.3.2 If the statement is made orally, Business Associate shall document the statement, including the identity of the official making the statement, and delay its reporting and/or notification obligation(s) temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in Section 5.3.1 is submitted during that time.

6. WRITTEN ASSURANCES OF SUBCONTRACTORS

6.1 In accordance with 45 C.F.R. § 164.502 (e)(1)(ii) and § 164.308 (b)(2), if applicable, Business Associate shall ensure that any Subcontractor that creates, receives, maintains, or transmits Protected Health Information on behalf of Business Associate is made aware of its status as a Business Associate with respect to such information and that Subcontractor agrees in writing to the same restrictions, conditions, and requirements that apply to Business Associate with respect to such information.

6.2 Business Associate shall take reasonable steps to cure any material breach or violation by Subcontractor of the agreement required by Section 6.1.

6.3 If the steps required by Section 6.2 do not cure the breach or end the violation, Contractor shall terminate, if feasible, any arrangement with Subcontractor by which Subcontractor creates, receives, maintains, or transmits Protected Health Information on behalf of Business Associate.

6.4 If neither cure nor termination as set forth in Sections 6.2 and 6.3 is feasible, Business Associate shall immediately notify County.

6.5 Without limiting the requirements of Section 6.1, the agreement required by Section 6.1 (Subcontractor Business Associate Agreement) shall require Subcontractor to contemporaneously notify Covered Entity in the event of a Breach of Unsecured Protected Health Information.

6.6 Without limiting the requirements of Section 6.1, agreement required by Section 6.1 (Subcontractor Business Associate Agreement) shall include a provision requiring Subcontractor to destroy, or in the alternative to return to Business Associate, any Protected Health Information created, received, maintained, or transmitted by Subcontractor on behalf of Business Associate so as to enable Business Associate to comply with the provisions of Section 18.4.

6.7 Business Associate shall provide to Covered Entity, at Covered Entity's request, a copy of any and all Subcontractor Business Associate Agreements required by Section 6.1.

6.8 Sections 6.1 and 6.7 are not intended by the parties to limit in any way the scope of Business Associate's obligations related to Subcontracts or Subcontracting in the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order, or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

7. ACCESS TO PROTECTED HEALTH INFORMATION

7.1 To the extent Covered Entity determines that Protected Health Information is maintained by Business Associate or its agents or Subcontractors in a Designated Record Set, Business Associate shall, within two (2) business days after receipt of a request from Covered Entity, make the Protected Health Information specified by Covered Entity available to the Individual(s) identified by Covered Entity as being entitled to access and shall provide such Individuals(s) or other person(s) designated by Covered Entity with a copy the specified Protected Health Information, in order for Covered Entity to meet the requirements of 45 C.F.R. § 164.524.

7.2 If any Individual requests access to Protected Health Information directly from Business Associate or its agents or Subcontractors, Business Associate shall notify Covered Entity in writing within two (2) days of the receipt of the request. Whether access shall be provided or denied shall be determined by Covered Entity.

7.3 To the extent that Business Associate maintains Protected Health Information that is subject to access as set forth above in one or more Designated Record Sets electronically and if the Individual requests an electronic copy of such information, Business

Associate shall provide the Individual with access to the Protected Health Information in the electronic form and format requested by the Individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by Covered Entity and the Individual.

8. AMENDMENT OF PROTECTED HEALTH INFORMATION

8.1 To the extent Covered Entity determines that any Protected Health Information is maintained by Business Associate or its agents or Subcontractors in a Designated Record Set, Business Associate shall, within ten (10) business days after receipt of a written request from Covered Entity, make any amendments to such Protected Health Information that are requested by Covered Entity, in order for Covered Entity to meet the requirements of 45 C.F.R. § 164.526.

8.2 If any Individual requests an amendment to Protected Health Information directly from Business Associate or its agents or Subcontractors, Business Associate shall notify Covered Entity in writing within five (5) days of the receipt of the request. Whether an amendment shall be granted or denied shall be determined by Covered Entity.

9. ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

9.1 Business Associate shall maintain an accounting of each Disclosure of Protected Health Information made by Business Associate or its employees, agents, representatives or Subcontractors, as is determined by Covered Entity to be necessary in order to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528.

9.1.1 Any accounting of disclosures provided by Business Associate under Section 9.1 shall include:

(a) The date of the Disclosure;

(b) The name, and address if known, of the entity or person who received the Protected Health Information;

(c) A brief description of the Protected Health Information Disclosed; and

(d) A brief statement of the purpose of the Disclosure.

9.1.2 For each Disclosure that could require an accounting under Section 9.1, Business Associate shall document the information specified in Section 9.1.1 and shall maintain the information for six (6) years from the date of the Disclosure.

9.2 Business Associate shall provide to Covered Entity, within ten (10) business days after receipt of a written request from Covered Entity, information collected in accordance with Section 9.1.1 to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528

9.3 If any Individual requests an accounting of disclosures directly from Business Associate or its agents or Subcontractors, Business Associate shall notify Covered Entity in writing within five (5) days of the receipt of the request, and shall provide the requested accounting of disclosures to the Individual(s) within 30 days. The information provided in the accounting shall be in accordance with 45 C.F.R. § 164.528.

10. COMPLIANCE WITH APPLICABLE HIPAA RULES

10.1 To the extent Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 C.F.R. Part 164, Business Associate shall comply with the requirements of Subpart E that apply to Covered Entity's performance of such obligation(s).

10.2 Business Associate shall comply with all HIPAA Rules applicable to Business Associate in the performance of Services.

10.3 Business Associate must demonstrate its compliance with Los Angeles County Board of Supervisors Policies and the requirements stated in this Business Associate Agreement Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Business Associate must attest that it has implemented adequate controls to meet the expected baseline set forth in Attachment XIV-__, Information Security Contract/Agreement Requirements, at the commencement and during the renewal of this agreement with the County. The completed Attachment XIII-__, DMH Business Associate/Contractor's Compliance with Information Security Requirements Exhibit questionnaire must be returned to DMH Information Security Officer (DISO) for approval within ten (10) business days from the signed date of this agreement and annually thereafter. Business Associate must be prepared to provide supporting evidence upon request.

10.4 During the term of the agreement, Business Associate must notify the Covered Entity within ten (10) days of implementation, in writing, about any significant changes such as technology changes, modification in the implemented security safeguards or any major infrastructure changes. Dependent on the adjustment, Business Associate may be asked to re-submit Attachment XIII-__, DMH Business Associate/Contractor's Compliance with Information Security Requirements Exhibit questionnaire, to document the change.

10.5 Business Associate must ensure that prior to access, workforce members including Subcontractors that create, receive, maintain, or transmit Protected Health Information on behalf of Business Associate or the County acknowledge and sign the Attachment X-__, the Confidentiality Oath (Non-LAC-DMH Workforce Members), to this agreement. Business Associate must maintain and make available upon request by the federal, State and/or County government.

11. AVAILABILITY OF RECORDS

11.1 Business Associate shall make its internal practices, books, and records relating to the Use and Disclosure of Protected Health Information received from or created or received by Business Associate on behalf of Covered Entity available to the Secretary for purposes of determining Covered Entity's compliance with the Privacy and Security Regulations.

11.2 Unless prohibited by the Secretary, Business Associate shall immediately notify Covered Entity of any requests made by the Secretary and provide Covered Entity with copies of any documents produced in response to such request.

12. MITIGATION OF HARMFUL EFFECTS

12.1 Business Associate shall mitigate, to the extent practicable, any harmful effect of a Use or Disclosure of Protected Health Information by Business Associate in violation of the requirements of this Business Associate Agreement that is known to Business Associate.

13. BREACH NOTIFICATION TO INDIVIDUALS

13.1 Business Associate shall, to the extent Covered Entity determines that there has been a Breach of Unsecured Protected Health Information by Business Associate, its employees, representatives, agents or Subcontractors, provide breach notification to the Individual in a manner that permits Covered Entity to comply with its obligations under 45 C.F.R. § 164.404.

13.1.1 Business Associate shall notify, subject to the review and approval of Covered Entity, each Individual whose Unsecured Protected Health Information has been, or is reasonably believed to have been, accessed, acquired, Used, or Disclosed as a result of any such Breach.

13.1.2 The notification provided by Business Associate shall be written in plain language, shall be subject to review and approval by Covered Entity, and shall include, to the extent possible:

(a) A brief description of what happened, including the date of the Breach and the date of the Discovery of the Breach, if known;

(b) A description of the types of Unsecured Protected Health Information that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

(c) Any steps the Individual should take to protect him or herself from potential harm resulting from the Breach;

(d) A brief description of what Business Associate is doing to investigate the Breach, to mitigate harm to Individual(s), and to protect against any further Breaches; and

(e) Contact procedures for Individual(s) to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

13.2 Covered Entity, in its sole discretion, may elect to provide the notification required by Section 13.1 and/or to establish the contact procedures described in Section 13.1.2.

13.3 Business Associate shall reimburse Covered Entity any and all costs incurred by Covered Entity, in complying with Subpart D of 45 C.F.R. Part 164, including but not limited to costs of notification, internet posting, or media publication, as a result of Business Associate's Breach of Unsecured Protected Health Information; Covered Entity shall not be responsible for any costs incurred by Business Associate in providing the notification required by 13.1 or in establishing the contact procedures required by Section 13.1.2.

14. INDEMNIFICATION

14.1 Business Associate shall indemnify, defend, and hold harmless Covered Entity, its Special Districts, elected and appointed officers, employees, and agents from and against any and all liability, including but not limited to demands, claims, actions, fees, costs, expenses (including attorney and expert witness fees), and penalties and/or fines (including regulatory penalties and/or fines), arising from or connected with Business Associate's acts and/or omissions arising from and/or relating to this Business Associate Agreement, including, but not limited to, compliance and/or enforcement actions and/or activities, whether formal or informal, by the Secretary or by the Attorney General of the State of California.

14.2 Section 14.1 is not intended by the parties to limit in any way the scope of Business Associate's obligations related to Insurance and/or Indemnification in the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order, or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

15. OBLIGATIONS OF COVERED ENTITY

15.1 Covered Entity shall notify Business Associate of any current or future restrictions or limitations on the Use or Disclosure of Protected Health Information that would affect Business Associate's performance of the Services, and Business Associate shall thereafter restrict or limit its own Uses and Disclosures accordingly.

15.2 Covered Entity shall not request Business Associate to Use or Disclose Protected Health Information in any manner that would not be permissible under Subpart E of 45 C.F.R. Part 164 if done by Covered Entity, except to the extent that Business Associate may Use or Disclose Protected Health Information as provided in Sections 2.3, 2.5, and 2.6.

16. TERM

16.1 Unless sooner terminated as set forth in Section 17, the term of this Business Associate Agreement shall be the same as the term of the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order, or other service arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

16.2 Notwithstanding Section 16.1, Business Associate's obligations under Sections 11, 14, and 18 shall survive the termination or expiration of this Business Associate Agreement.

17. TERMINATION FOR CAUSE

17.1 In addition to and notwithstanding the termination provisions set forth in the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order, or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate, if either party determines that the other party has violated a material term of this Business Associate Agreement, and the breaching party has not cured the breach or ended the violation within the time specified by the non-breaching party, which shall be reasonable given the nature of the breach and/or violation, the non-breaching party may terminate this Business Associate Agreement.

17.2 In addition to and notwithstanding the termination provisions set forth in the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order, or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate, if either party determines that the other party has violated a material term of this Business Associate Agreement, and cure is not feasible, the non-breaching party may terminate this Business Associate Agreement immediately.

18. DISPOSITION OF PROTECTED HEALTH INFORMATION UPON TERMINATION OR EXPIRATION

18.1 Except as provided in Section 18.3, upon termination for any reason or expiration of this Business Associate Agreement, Business Associate shall return or, if agreed to by Covered entity, shall destroy as provided for in Section 18.2, all Protected Health Information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, that Business Associate, including any Subcontractor, still maintains in any form. Business Associate shall retain no copies of the Protected Health Information.

18.2 Destruction for purposes of Section 18.2 and Section 6.6 shall mean that media on which the Protected Health Information is stored or recorded has been destroyed and/or electronic media have been cleared, purged, or destroyed in accordance with the use of a technology or methodology specified by the Secretary in guidance for rendering Protected Health Information unusable, unreadable, or indecipherable to unauthorized individuals.

18.3 Notwithstanding Section 18.1, in the event that return or destruction of Protected Health Information is not feasible or Business Associate determines that any such Protected Health Information is necessary for Business Associate to continue its proper

management and administration or to carry out its legal responsibilities, Business Associate may retain that Protected Health Information for which destruction or return is infeasible or that Protected Health Information which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities and shall return or destroy all other Protected Health Information.

18.3.1 Business Associate shall extend the protections of this Business Associate Agreement to such Protected Health Information, including continuing to use appropriate safeguards and continuing to comply with Subpart C of 45 C.F.R Part 164 with respect to Electronic Protected Health Information, to prevent the Use or Disclosure of such information other than as provided for in Sections 2.5 and 2.6 for so long as such Protected Health Information is retained, and Business Associate shall not Use or Disclose such Protected Health Information other than for the purposes for which such Protected Health Information was retained.

18.3.2 Business Associate shall return or, if agreed to by Covered entity, destroy the Protected Health Information retained by Business Associate when it is no longer needed by Business Associate for Business Associate's proper management and administration or to carry out its legal responsibilities.

18.4 Business Associate shall ensure that all Protected Health Information created, maintained, or received by Subcontractors is returned or, if agreed to by Covered entity, destroyed as provided for in Section 18.2.

19. AUDIT, INSPECTION, AND EXAMINATION

19.1 Covered Entity reserves the right to conduct a reasonable inspection of the facilities, systems, information systems, books, records, agreements, and policies and procedures relating to the Use or Disclosure of Protected Health Information for the purpose determining whether Business Associate is in compliance with the terms of this Business Associate Agreement and any non-compliance may be a basis for termination of this Business Associate Agreement and the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate, as provided for in section 17.

19.2 Covered Entity and Business Associate shall mutually agree in advance upon the scope, timing, and location of any such inspection.

19.3 At Business Associate's request, and to the extent permitted by law, Covered Entity shall execute a nondisclosure agreement, upon terms and conditions mutually agreed to by the parties.

19.4 That Covered Entity inspects, fails to inspect, or has the right to inspect as provided for in Section 19.1 does not relieve Business Associate of its responsibility to comply with this Business Associate Agreement and/or the HIPAA Rules or impose on Covered Entity any responsibility for Business Associate's compliance with any applicable HIPAA Rules.

19.5 Covered Entity's failure to detect, its detection but failure to notify Business Associate, or its detection but failure to require remediation by Business Associate of an unsatisfactory practice by Business Associate, shall not constitute acceptance of such practice or a waiver of Covered Entity's enforcement rights under this Business Associate Agreement or the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

19.6 Section 19.1 is not intended by the parties to limit in any way the scope of Business Associate's obligations related to Inspection and/or Audit and/or similar review in the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order, or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

20. MISCELLANEOUS PROVISIONS

20.1 Disclaimer. Covered Entity makes no warranty or representation that compliance by Business Associate with the terms and conditions of this Business Associate Agreement will be adequate or satisfactory to meet the business needs or legal obligations of Business Associate.

20.2 HIPAA Requirements. The Parties agree that the provisions under HIPAA Rules that are required by law to be incorporated into this Amendment are hereby incorporated into this Agreement.

20.3 No Third Party Beneficiaries. Nothing in this Business Associate Agreement shall confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

20.4 Construction. In the event that a provision of this Business Associate Agreement is contrary to a provision of the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order, or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate, the provision of this Business Associate Agreement shall control. Otherwise, this Business Associate Agreement shall be construed under, and in accordance with, the terms of the applicable underlying Agreement, Contract, Master Agreement, Work Order, Purchase Order or other services arrangement, with or without payment, that gives rise to Contractor's status as a Business Associate.

20.5 Regulatory References. A reference in this Business Associate Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

20.6 Interpretation. Any ambiguity in this Business Associate Agreement shall be resolved in favor of a meaning that permits the parties to comply with the HIPAA Rules.

20.7 Amendment. The parties agree to take such action as is necessary to amend this Business Associate Agreement from time to time as is necessary for Covered Entity or Business Associate to comply with the requirements of the HIPAA Rules and any other privacy laws governing Protected Health Information.

/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/
/

COUNTY OF LOS ANGELES

By

Jonathan E. Sherin, M.D., Ph. D.	Director of Mental Health
Authorized Signatory Name	**Authorized Signatory Title**

Authorized Signatory Signature	**Date**

BUSINESS ASSOCIATE

By

Authorized Signatory Name	**Authorized Signatory Title**

Authorized Signatory Signature	**Date**

DMH BUSINESS ASSOCIATE / CONTRACTOR'S COMPLIANCE
WITH INFORMATION SECURITY REQUIREMENTS EXHIBIT

Business Associate / Contractor Agency Name: _____

Business Associate / Contractor shall provide information about its information security practices by completing this Exhibit **annually**. By submitting this Exhibit, Business Associate / Contractor certifies that will be compliant with Los Angeles County Board of Supervisors Policies and attest that it has implemented adequate controls to meet the following expected Information Security minimum standard, at the commencement and during the term of any awarded agreement. Business Associate must be prepared to provide supporting evidence upon request. The completed forms must be returned to DMH Information Security Officer (DISO) for approval within ten (10) business days from the signed date of this agreement. Any significant changes during the term of the contract/agreement must be reported within ten (10) business days of implementation. Dependent on the adjustment, Business Associate / Contractor may be asked to re-submit this exhibit to document the change.

COMPLIANCE QUESTIONS

						DOCUMENTATION AVAILABLE		
		YES	NO	N/A		YES	NO
1	Will County's non-public data stored on your workstation(s) be encrypted? *If "NO", or N/A please explain.*	☐	☐	☐		☐	☐
		YES	NO	N/A		YES	NO
2	Will County data stored on your laptop(s) be encrypted? *If "NO", or N/A please explain.*	☐	☐	☐		☐	☐
		YES	NO	N/A		YES	NO
3	Will County non-public data stored on removable media be encrypted? *If "NO", or N/A please explain.*	☐	☐	☐		☐	☐
		YES	NO	N/A		YES	NO
4	Will County data be encrypted when transported? *If "NO", or N/A please explain.*	☐	☐	☐		☐	☐
		YES	NO	N/A		YES	NO
5	Will you maintain a copy of any validation / attestation reports generated by its encryption tools? *If "NO", or N/A please explain.*	☐	☐	☐		☐	☐
		YES	NO	N/A		YES	NO
6	Will County data be stored on remote servers*? *Cloud storage, Software-as-a-Service or SaaS *Please provide public URL and hosting information for the server.*	☐	☐	☐		☐	☐
		YES	NO	N/A		YES	NO
7	Will all users with access to County data participate in an annual information security awareness training? *If "NO", or N/A please explain.*	☐	☐	☐		☐	☐
		YES	NO	N/A		YES	NO
8	Will County data residing on endpoints be protected by an up-to-date antivirus and/or anti-malware software? *If "NO", or N/A please explain.*	☐	☐	☐		☐	☐
		YES	NO	N/A		YES	NO

To be completed and returned to DMH Information Security Officer within ten (10) business days from the signed date of this agreement

9	Will all endpoints accessing and/or storing County data be physically secured? *If "NO", or N/A please explain.*	☐	☐	☐	☐	☐
		YES	**NO**	**N/A**	**YES**	**NO**
10	Will all security incidents involving County data be promptly reported? *If "NO", or N/A please explain.*	☐	☐	☐	☐	☐
		YES	**NO**	**N/A**	**YES**	**NO**
11	Will all users' access be formally authorized, and users provided with unique logon IDs & complex passwords for accessing County data? *If "NO", or N/A please explain.*	☐	☐	☐	☐	☐
		YES	**NO**	**N/A**	**YES**	**NO**
12	Will all users' activities be monitored to ensure they are accessing the minimum information necessary to perform their assignments? *If "NO", or N/A please explain.*	☐	☐	☐	☐	☐
		YES	**NO**	**N/A**	**YES**	**NO**
13	Will users' access be modified once their role no longer justifies such access or access promptly suspended upon discharge/termination? *If "NO", or N/A please explain.*	☐	☐	☐	☐	☐
		YES	**NO**	**N/A**	**YES**	**NO**
14	Will all endpoints accessing and/or storing County data be regularly patched and updated for known vulnerabilities? *If "NO", or N/A please explain.*	☐	☐	☐	☐	☐
		YES	**NO**	**N/A**	**YES**	**NO**
15	Will all endpoints accessing and/or storing County data be rendered unreadable and/or unrecoverable, prior to disposition? *If "NO", or N/A please explain.*	☐	☐	☐	☐	☐
		YES	**NO**	**N/A**	**YES**	**NO**
16	Will Business Associate / Contractor inspect and conduct annual risk assessments on its systems involving County data to identify and mitigate weaknesses and vulnerabilities? *If "NO", or N/A please explain.*	☐	☐	☐	☐	☐
		YES	**NO**	**N/A**	**YES**	**NO**
17	Does the entity have policies and procedures to ensure continuity and availability of critical business processes during emergencies or disasters and ability to restore/recover data from ransomware attacks? *If "NO", or N/A please explain.*	☐	☐	☐	☐	☐
		YES	**NO**	**N/A**	**YES**	**NO**
18	Will Business Associate / Contractor return or destroy non-public County data upon expiration or termination of their contract? *If "NO", or N/A please explain.*	☐	☐	☐	☐	☐

Authorized Signatory Name (Print) | **Authorized Signatory Official Title**

Authorized Signatory Signature | **Date**

To be completed and returned to DMH Information Security Officer within ten (10) business days from the signed date of this agreement

INFORMATION SECURITY CONTRACT/AGREEMENT REQUIREMENTS

This Attachment sets forth information security requirements and procedures to be established by Contractor/Business Associate before the effective date of the Contract/Agreement and maintained throughout the term of the Contract/Agreement. These requirements and procedures are a minimum standard and are in addition to the requirements of the Contract/Agreement and any other Arrangements between the parties. However, it is Contractor/Business Associate's sole obligation to: (i) implement appropriate measures to secure its systems and all Information (as defined by County Board of Supervisors Policy 6.104), against internal and external threats and risks; and (ii) continuously review and revise those measures to address ongoing threats and risks. Failure to comply with the minimum requirements and procedures set forth in this Attachment will constitute a material, non-curable breach of the Contract/Agreement by Contractor/Business Associate, entitling County, in addition to and cumulative of all other remedies available to it at law, in equity, or under the Contract/Agreement, to immediately terminate the Contract/Agreement. Unless specifically defined in this Attachment, capitalized terms shall have the meanings set forth in the Contract/Agreement.

1. NON-EXCLUSIVE EQUITABLE REMEDY

Contractor/Business Associate acknowledges and agrees that due to the unique nature of County Non Public Information (NPI) there can be no adequate remedy at law for any breach of its obligations hereunder, that any such breach may result in irreparable harm to County, and therefore, that upon any such breach, County will be entitled to appropriate equitable remedies, and may seek injunctive relief from a court of competent jurisdiction without the necessity of proving actual loss, in addition to whatever remedies either of them might have at law or equity. Any breach of Section 5 (Confidentiality) shall constitute a material breach of this Contract/Agreement and be grounds for immediate termination of this Contract/Agreement in the exclusive discretion of the County.

2. INFORMATION SECURITY PROGRAM

Contractor/Business Associate shall establish and maintain a company-wide Information Security Program (Information Security Management System [ISMS]) designed to evaluate risks to the confidentiality, availability and integrity of the information in their possession.

Contractor/Business Associate's Information Security Program shall include the creation and maintenance of security policies, standards and procedures (collectively "**Information Security Policy**"). The Information Security Policy will be communicated to all Contractor/Business Associate personnel in a relevant, accessible, and understandable form and will be regularly reviewed and evaluated to ensure its operational effectiveness, compliance with all applicable laws and regulations, and to address new threats/risks.

3. PROPERTY RIGHTS TO INFORMATION

All Information, as defined by County Board of Supervisors Policy 6.104 - Information Classification Policy, provided for the County or collected by Contractor/Business Associate on behalf of the County, is deemed property of the County and shall remain the property of County and County shall retain exclusive rights and ownership thereto.

The County Information shall not be used by Contractor/Business Associate for any purpose other than as required under this Contract/Agreement, nor shall such information or any part of such information be disclosed, sold, assigned, leased, or otherwise disposed of to third-parties by Contractor/Business Associate or commercially exploited or otherwise used by, or on behalf of, Contractor/Business Associate, its officers, directors, employees, or agents. Contractor/Business Associate may assert no lien on or right to withhold from County, any information it receives from, receives addressed to, or stores on behalf of, County.

Notwithstanding the foregoing, Contractor/Business Associate may aggregate, compile, and use County Information in order to improve, develop or enhance the System Software and/or other services offered, or to be offered, by Contractor/Business Associate; provided that no County Information in such aggregated or compiled pool is identifiable as originating from, or can be traced back to, County or a County, and such Information cannot be associated or matched with an identifiable profile or personally identifiable information. Contractor/Business Associate specifically consents to the County's access to such County Information held, stored, or maintained on any and all devices Contactor owns, leases or possesses.

4. CONTRACTOR/BUSINESS ASSOCIATE'S USE OF INFORMATION

Contractor/Business Associate may use the Information only as necessary to carry out its obligations under this Contract/Agreement, and for no other purpose other than observation and reporting to the County on County's usage of the Information and making recommendations for improved usage.

5. CONFIDENTIALITY

a) Non-public Information. Contractor/Business Associate agrees that all information supplied by its affiliates and agents to the County including, without limitation, (a) any information relating to County's customers, patients, business partners, or personnel; (b) Personally Identifiable Information (as defined below); (c) any non- public information as defined in the Gramm-Leach-Bliley Act or the California Financial Information Privacy Act, and (d) any Protected Health Information as defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and The Health Information Technology for Economic and Public Health Act (HITECH), will be deemed confidential and proprietary to the County, regardless of whether such information was disclosed intentionally or unintentionally or marked as "confidential". To be deemed "Non-public Information" (NPI) as defined in Board of Supervisors Policy 6.104 – Information Classification Policy, trade secrets and mask works must be plainly and prominently marked with restrictive legends.

b) Nondisclosure of NPI. NPI provided by the County either before or after Contract/Agreement award shall only be used for its intended purpose. Contractor/Business Associate and Subcontractors shall not utilize nor distribute County NPI in any form without the prior express written approval of the County.

c) Non-Disclosure Obligation. While performing work under this Contract/Agreement, the Contractor/Business Associate and Subcontractors may encounter NPI such as personal information, licensed technology, drawings, schematics, manuals, sealed court records, and other materials described as "Internal Use", "Confidential" or "Restricted" as defined in Board of Supervisors Policy 6.104 – Information Classification Policy as NPI. The Contractor/Business Associate shall not disclose or publish any information and material received or used in performance of this Contract/Agreement. This obligation is perpetual. The Contract/Agreement imposes no obligation upon the Contractor/Business Associate with respect to County NPI which the Contractor/Business Associate can establish that: a) was in the possession of, or was rightfully known by the Contractor/Business Associate without an obligation to maintain its confidentiality prior to receipt from the County or a third party; b) is or becomes generally known to the public without violation of this Contract/Agreement; c) is obtained by the Contractor/Business Associate in good faith from a third party having the right to disclose it without an obligation of confidentiality; or, d) is independently developed by the Contractor/Business Associate without the participation of individuals who have had access to the County's or the third party's NPI. If the Contractor/Business Associate is required by law to disclose NPI the Contractor/Business Associate shall notify the County of such requirement prior to disclosure.

d) Personally Identifiable Information. "Personally Identifiable Information" (PII) shall mean any information about an individual maintained by an organization or other entity, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

In connection with this Contract/Agreement and performance of the services, Contractor/Business Associate may be provided or obtain, from County or otherwise, PII pertaining to County's current and prospective personnel, directors and officers, agents, investors, patients, and customers and may need to process such PII and/or transfer it, all subject to the restrictions set forth in this Contract/Agreement and otherwise in compliance with all applicable foreign and domestic laws and regulations for the sole purpose of performing the services.

e) Treatment of County Non-public Information. Without limiting any other warranty or obligations specified in this Contract/Agreement, and in particular the Confidentiality provisions of the Contract/Agreement, during the term of this Contract/Agreement and thereafter in perpetuity, Contractor/Business Associate will not gather, store, log, archive, use, or otherwise retain any County NPI in any manner and will not disclose, distribute, sell, share, rent, or otherwise retain any County NPI to any third-party, except as expressly required to perform its obligations under this Contract/Agreement or as Contractor/Business Associate may be expressly directed in advance in writing by County.

Contractor/Business Associate represents and warrants that Contractor/Business Associate will use and process County NPI only in compliance with (a) this Contract/Agreement, (b) County's then current information security and privacy policies, and (c) all applicable County, state, and federal laws and regulations.

f) Retention of County Non-public Information. Contractor/Business Associate will not retain any County NPI for any period longer than necessary for Contractor/Business Associate to fulfill its obligations under this Contract/Agreement or required by Contractor/Business Associate's records retention policies and applicable law.

g) Return of County Non-public Information. On County's written request or upon expiration or termination of this Contract/Agreement for any reason, Contractor/Business Associate will promptly return or destroy, at County's option, all originals and copies of all documents and materials it has received containing County's NPI; (b) if return or destruction is not permissible under applicable law, continue to protect such information in accordance with the terms of this Contract/Agreement; and (c) deliver or destroy, at County's option, all originals and copies of all summaries, records, descriptions, modifications, negatives, drawings, adoptions and other documents or materials, whether in writing or in machine-readable form, prepared by Contractor/Business Associate, prepared under its direction, or at its request, from the documents and materials referred to in Subsection 5(a) of this Attachment, and provide a notarized written statement to County certifying that all documents and materials referred to in Subsections 5(a) and (b) of this Attachment have been delivered to County or destroyed, as requested by County.

On termination or expiration of this Contract/Agreement, County will return or destroy all Contractor/Business Associate's information marked as confidential (excluding items licensed to County hereunder or that provided to County by Contractor/Business Associate hereunder), at County's option.

6. CONTRACTOR/BUSINESS ASSOCIATE PERSONNEL

Within the limitations of law, Contractor/Business Associate shall screen and conduct background investigations on all Contractor/Business Associate personnel, Contractor/Business Associates and third-parties as appropriate to their role, with actual or potential physical or logical access to County's NPI for potential security risks. Such background investigations, based on the individual's role and interaction with NPI, may include criminal and financial history and will be repeated on a regular basis.

Contractor/Business Associate shall require all employees and Contractor/Business Associate s to sign an appropriate written confidentiality/non- disclosure agreement.

All agreements with third-parties involving access to Contractor/Business Associate's systems and Information, including all outsourcing arrangements and maintenance and support agreements (including facilities maintenance), shall specifically address security risks, controls, and procedures for information systems.

Contractor/Business Associate shall supply each of its Contractor/Business Associate personnel with appropriate, ongoing training regarding information security procedures, risks, and threats.

Contractor/Business Associate shall have an established set of procedures to ensure Contractor/Business Associate personnel promptly report actual and/or suspected breaches of security.

7. STORAGE, TRANSMISSION AND DESTRUCTION OF COUNTY NON-PUBLIC INFORMATION

All County NPI shall be rendered unusable, unreadable, or indecipherable to unauthorized individuals. Without limiting the generality of the foregoing, Contractor/Business Associate will encrypt all workstations, portable devices (e.g., mobile, wearables, tablets,) and removable media (portable or removable hard disks, floppy disks, USB memory drives, CDs, DVDs, magnetic tape, and all other removable storage media) that store County's NPI in accordance with Federal Information Processing Standard (FIPS) 140-2 or otherwise approved by the County's Chief Information Security Officer.

8. HARDWARE RETURN

Upon termination or expiration of the Contract/Agreement or at any time upon County's request, Contractor/Business Associate shall return all hardware, if any, provided by County to County.

The hardware should be physically sealed and returned via a bonded courier or as otherwise directed by County.

9. PHYSICAL AND ENVIRONMENTAL SECURITY

Contractor/Business Associate facilities that process County Information will be housed in secure areas and protected by perimeter security such as barrier access controls (e.g., the use of guards and entry badges) that provide a physically secure environment from unauthorized access, damage, and interference.

Contractor/Business Associate facilities that process County Information will be maintained with physical and environmental controls (temperature and humidity) that meet or exceed hardware manufacturer's specifications.

10. COMMUNICATIONS AND OPERATIONAL MANAGEMENT

Contractor/Business Associate shall: (i) monitor and manage all of its information processing facilities, including, without limitation, implementing operational procedures, change management and incident response procedures; and (ii) deploy adequate anti-malware software and adequate back-up systems to ensure essential business information can be promptly recovered in the event of a disaster or media failure; and (iii) ensure its operating procedures are adequately documented and designed to protect information and computer media from theft and unauthorized access.

11. ACCESS CONTROL

Subject to and without limiting the requirements under Section 7 (Storage, Transmission and Destruction of Information), County's NPI: (i) may only be made available and accessible to those parties explicitly authorized under the Contract/Agreement or otherwise expressly approved by County in writing; (ii) if transferred across the Internet, any wireless network (e.g., cellular, 802.11x, or similar technology), or other public or shared networks, must be protected using appropriate encryption technology as designated or approved by County's Chief Information Security Officer in writing; and (iii) if transferred using Removable Media (as defined above) must be sent via a bonded courier and protected using encryption technology designated by Contractor/Business Associate and approved by County's Chief Information Security Officer in writing. The foregoing requirements shall apply to back-up media stored by Contractor/Business Associate at off-site facilities.

Contractor/Business Associate shall implement formal procedures to control access to County systems, services, and/or data, including, but not limited to, user account management procedures and the following controls:

a) Network access to both internal and external networked services shall be controlled, including, but not limited to, the use of properly configured firewalls;

b) Operating systems will be used to enforce access controls to computer resources including, but not limited to, authentication, authorization, and event logging;

c) Applications will include access control to limit user access to information and application system functions; and

d) All systems will be monitored to detect deviation from access control policies and identify suspicious activity. Contractor/Business Associate shall record, review and act upon all events in accordance with incident response policies set forth below.

In the event any hardware, storage media, or removable media must be disposed of or sent off-site for servicing, Contractor/Business Associate shall ensure all County NPI, has been cleared, purged, or scrubbed from such hardware and/or media using industry best practices as discussed in Section 7 (Storage. Transmission and Destruction of County Non-Public Information).

12. SECURITY INCIDENT

A "Security Incident" shall mean the successful unauthorized access, use, disclosure, or modification of

County NPI or interference with system operations in an information system.

a) Contractor/Business Associate will promptly notify, within three (3) business days after the detection, the County's Chief Information Security Officer by telephone and subsequently via written letter of any Security Incidents.

b) The notice shall include the approximate date and time of the occurrence and a summary of the relevant facts, including a description of measures being taken to address the occurrence. Contractor/Business Associate will

provide a quarterly report of all Security Incidents noting the actions taken. This will be provided via a written letter to the County's Chief Information Security Officer on or before the first (1st) week of each calendar quarter (January, March, June and September). County or its third-party designee may, but is not obligated to, perform audits and security tests of Contractor/Business Associate's environment that may include, but are not limited to, interviews of relevant personnel, review of documentation, or technical inspection of systems, as they relate to the receipt, maintenance, use, retention, and authorized destruction of County NPI.

c) Notwithstanding any other provisions in this Contract/Agreement, Contractor/Business Associate shall be liable for all damages, fines, corrective action and legally required notifications arising from a security incident that results in unauthorized access, modification, destruction or compromise of County Information caused by Contractor/Business Associate's weaknesses, negligence, errors, or lack of information security or privacy controls or provisions hereunder.

13. AUDIT

When not prohibited by regulation, Contractor/Business Associate will provide to County a summary of: (1) the results of any security audits, security reviews, or other relevant audits, conducted by Contractor/Business Associate or a third party; and (2) corrective actions or modifications, if any, Contractor/Business Associate will implement in response to such audits.

During the term of this Contract/Agreement, County or a mutually agreed third-party designee may annually, or more frequently as agreed in writing by the parties, request a security audit of Contractor/Business Associate's Information Security Management System (ISMS), data center, services and/or systems containing or processing County Information.

The audit will take place at a time mutually agreed to by the parties, but in no event on a date more than ninety (90) days from the date of the request by County.

County's request for security audit will specify the scope and areas (e.g., Administrative, Physical and Technical) that are subject to the audit and may include but not limited to physical controls inspection, process reviews, policy reviews evidence of external and internal vulnerability scans, penetration tests results, evidence of code reviews, and evidence of system configuration and audit log reviews. County shall pay for all third-party costs associated with the audit. It is understood that the results may be filtered to remove the specific information of other Contractor/Business Associate customers such as IP address, server names, etc.

Contractor/Business Associate shall cooperate with County in the development of the scope and methodology for the audit, and the timing and implementation of the audit. Any of the County's regulators shall have the same right upon request, to request an audit as described above. Contractor/Business Associate agrees to comply with all reasonable recommendations that result from such inspections, tests, and audits within reasonable timeframes.

14. SPECIFIC SOFTWARE AS A SERVICE (SaaS) CONTRACTUAL TERMS AND CONDITIONS

a) License. Subject to the terms and conditions set forth in this Contract/Agreement, including payment of the license fees by County to Contractor/Business Associate, Contractor/Business Associate hereby grants to County a non-exclusive, non-transferable worldwide license to use the service during the term of this Contract/Agreement to achieve the purposes stated herein, as well as any documentation and training materials.

b) Business Continuity. In the event that Contractor/Business Associate's infrastructure or Information becomes lost, damaged or destroyed, Contractor/Business Associate shall immediately, and not longer than one (1) business day, implement the Contractor/Business Associate's Business Continuity Plan, in order to continue to provide the service. Contractor/Business Associate's obligation to reimburse the County's costs related to lost, damaged or destroyed Information shall be determined by the County.

The plan, at a minimum, shall include the services of a third-party recovery provider for which the County shall be the first in the order of recovery among Contractor/Business Associate's customers. The third-party recovery provider shall provide and assist Contractor/Business Associate in its operations, system management and technical support.

The Contractor/Business Associate shall include in its Business Continuity Plan a service offering, a distributed IT infrastructure and a mirrored critical system, Contractor/Business Associate will assist the County in providing such a system within one (1) Day of the County's notification.

In the event that the service is interrupted, the Information may be accessed and retrieved within two (2) hours at any point in time. Additionally, Contractor/Business Associate shall store a backup of all Information in an off-site "hardened" facility no less than daily, maintaining the security of Information, the security requirements of which are described herein.

c) Enhancements, Upgrades, Replacements and New Versions. The Contractor/Business Associate agrees to Provide to the County, at no cost, prior to, and during installation and implementation of the system any Software/firmware Enhancements, Upgrades and replacements which the Contractor/Business Associate initiates or generates that are within the scope of the products licensed and that are made available at no charge to other Contractor/Business Associate customers.

During the term of this Contract/Agreement, the Contractor/Business Associate shall notify the County of the availability of newer versions of the software and within thirty (30) Days provide the County with this new version.

The Contractor/Business Associate shall provide any Updated Documentation in the form of new revision manuals or changed pages to current manuals consistent with the original Documentation supplied and reflecting the changes included in the new version of the software as they are made available. The Contractor/Business Associate shall also provide installation instructions, procedures and any installation program required by the Enhancement, Upgrade, Replacement or new versions.

During the Contract/Agreement term, Contractor/Business Associate shall not delete or disable a feature or functionality unless the Contractor/Business Associate provides sixty (60) Days advance notice and the County provides written consent to the deleted or disabled feature or functionality. Should there be a replacement feature or functionality, the County shall have the sole discretion whether to accept such replacement. The replacement shall be at no additional cost to the County.

d) Contractor/Business Associate's Use of Information. Contractor/Business Associate may use the Information only as necessary to carry out its obligations under this Contract/Agreement, and for no other purpose other than the following:

i) May observe and report back to the County on County's usage of the service and make recommendations for improved usage.

e) Disposition of Information; Back-up Information. County retains the right to use the service to access and retrieve County content and data stored on Contractor/Business Associate's infrastructure at its sole discretion.

Contractor/Business Associate shall back up Information once in each 24-hour period.

f) Location of Information. Contractor/Business Associate warrants and represents that it shall store and process County Information and content only in the continental United States and that at no time will County Information traverse the borders of the continental United States in an unencrypted manner.

g) Data Center Audit and Certification. An SOC 3 audit certification shall be conducted annually, and a copy of the results provided to the County both during and prior to the commencement of the Contract/Agreement. The results of the SOC 3 audit and Contractor/Business Associate's plan for addressing or resolving the audit findings shall be shared with the County within ten (10) business days of Contractor/Business Associate's receipt of the audit results. Contractor/Business Associate agrees to provide the County with the current SOC 2 or any comparable compliance certification upon the County's request.

At its own expense, the County shall have the right to confirm Contractor/Business Associate's infrastructure and security practices via an onsite inspection at least once a year. In lieu of an on-site audit and upon the County's request, Contractor/Business Associate shall complete an audit questionnaire regarding Contractor/Business Associate's information security program.

h) Services Provided by a Subcontractor. Prior to the use of any Subcontractor for SaaS services under this Contract/Agreement, Contractor/Business Associate shall notify the County of the Subcontractor(s) that will be involved in providing any services to the County and obtain the County's written consent.

In the event that Contractor/Business Associate terminates its agreement with the Subcontractor, Contractor/Business Associate shall first allow the County to assume all of the rights and obligations of Contractor/Business Associate under the agreement and to transfer the agreement to the County, provided there shall be no changes in the services requirement. Contractor/Business Associate shall provide the County with advance written notice of its intent to terminate the Subcontractor agreement and at least thirty (30) Days to respond and indicate whether the County wishes to assume the rights and obligations under the Subcontractor agreement.

i) Information Import Requirements at Termination. Within one (1) Day of notification of termination of this Contract/Agreement, the Contractor/Business Associate shall provide the County with a complete and secure copy of all County Information suitable for import into commercially available database software (e.g. MS-SQL), such as XML format, including all schema and transformation definitions and/or delimited text files with documented, detailed schema definitions along with attachments in their native format. These files will be comprised of data contained in the Contractor/Business Associate's system. The structure of the relational database will be specific to the data and will not be representative of the proprietary Contractor/Business Associate database.

j) Termination Assistance Services. During the ninety (90) Day period prior to, and or following the expiration or termination of this Contract/Agreement, in whole or in part, Contractor/Business Associate agrees to provide reasonable termination assistance services at no additional cost to the County, which may include:

- **i)** Developing a plan for the orderly transition of the terminated or expired SaaS from Contractor/Business Associate to the successor;
- **ii)** Providing reasonable training to County staff or the successor in the performance of the SaaS then being performed by Contractor/Business Associate;
- **iii)** Using its best efforts to assist and make available to County any third-party services then being used by Contractor/Business Associate in connection with the SaaS; and
- **iv)** Such other activities upon which the parties may agree.

15. CERTIFICATION

The County must receive within ten (10) business days of its request, a certification from Contractor/Business Associate (for itself and any Subcontractors) that certifies and validates compliance with the minimum standard set forth above. In addition, Contractor/Business Associate shall maintain a copy of any validation/attestation reports that its product(s) generate, and such reports shall be subject to audit in accordance with the agreement. Failure on the part of the Contractor/Business Associate to comply with any of the provisions of this Attachment, Information Security Contract/Agreement Requirements shall constitute a material breach of this arrangement upon which the County may terminate or suspend this agreement.

16. REPORTING REQUIREMENTS FOR SIGNIFICANT CHANGES

During the term of this contract/agreement, Contractor/Business Associate must notify the Covered Entity within ten (10) days of implementation, in writing, about any significant changes such as technology changes, modification in the implemented security safeguards or any major infrastructure changes. Dependent on the adjustment, Contractor/Business Associate may be asked to re-submit the Attachment III - __ to document the change.

17. COMPLIANCE

Contractor/Business Associate shall provide information about its information security practices by completing Attachment III - _ "DMH Business Associate/ Contractor's Compliance with Information Security Requirements Attachment" questionnaire. By submitting, Contractor/Business Associate certifies that it will be in compliance with Los Angeles County Board of Supervisors Policies, and the expected minimum standard set forth above at the commencement of this agreement with the County and during the term of any arrangement that may be awarded pursuant to this agreement. The completed forms must be returned to DMH Information Security Officer (DISO) within ten (10) business days and approved to certify compliance.

COUNTY OF LOS ANGELES - DEPARTMENT OF MENTAL HEALTH

APPROVAL TO EXTEND THE TERM OF 29 EXISTING FEE-FOR-SERVICE MEDI-CAL ACUTE PSYCHIATRIC INPATIENT HOSPITAL SERVICES AGREEMENTS AND TWO SOLE SOURCE INDIGENT ACUTE PSYCHIATRIC INPATIENT HOSPITAL SERVICES AGREEMENTS

#	Acute Psychiatric Inpatient Hospital DBA Name (Corporation Name)	Supervisorial District	Service Area	Type of Hospital	FFS Medi-Cal Hospital	Sole Source Indigent Hospital
1	Adventist Health Glendale (Adventist Health) 1509 Wilson Terrace Glendale, CA 91206	5	2	GACH	X	
2	Adventist Health White Memorial (Adventist Health) 1720 E. Cesar Chavez Ave Los Angeles, CA 90033	1	4	GACH	X	
3	Antelope Valley Hospital (Antelope Valley Healthcare District) 1600 West Avenue J Lancaster, CA 93534	5	1	GACH	X	
4	Aurora Charter Oak (Aurora Charter Oak Hospital LLC) 1161 E. Covina Blvd Covina, CA 91724	5	3	APH	X	X
5	Aurora Las Encinas Hospital (Aurora Las Encinas Hospital LLC) 2900 E. Del Mar Blvd Pasadena, CA 91102	5	3	APH	X	

APH: Acute Psychiatric Hospital ***GACH:*** General Acute Care Hospital

COUNTY OF LOS ANGELES - DEPARTMENT OF MENTAL HEALTH

APPROVAL TO EXTEND THE TERM OF 29 EXISTING FEE-FOR-SERVICE MEDI-CAL ACUTE PSYCHIATRIC INPATIENT HOSPITAL SERVICES AGREEMENTS AND TWO SOLE SOURCE INDIGENT ACUTE PSYCHIATRIC INPATIENT HOSPITAL SERVICES AGREEMENTS

#	Acute Psychiatric Inpatient Hospital DBA Name (Corporation Name)	Supervisorial District	Service Area	Type of Hospital	FFS Medi-Cal Hospital	Sole Source Indigent Hospital
6	BHC Alhambra Hospital (BHC Alhambra Hospital, Inc.) 4619 N. Rosemead Blvd Rosemead, CA 91770	1	3	APH	X	
7	College Hospital Cerritos (College Hospital Inc.) 10802 College Place Cerritos, CA 90703	4	7	APH	X	X
8	College Hospital Costa Mesa (College Hospital Inc.) 301 Victoria Street Costa Mesa, CA 92627	OOC	OOC	GACH	X	
9	College Medical Center (CHLB, LLC) 2776 Pacific Ave Long Beach, CA 90806	4	8	GACH	X	
10	Del Amo Hospital, Inc. 23700 Camino Del Sol Torrance, CA 90505	4	8	APH	X	

APH: Acute Psychiatric Hospital ***GACH:*** General Acute Care Hospital

COUNTY OF LOS ANGELES - DEPARTMENT OF MENTAL HEALTH

APPROVAL TO EXTEND THE TERM OF 29 EXISTING FEE-FOR-SERVICE MEDI-CAL ACUTE PSYCHIATRIC INPATIENT HOSPITAL SERVICES AGREEMENTS AND TWO SOLE SOURCE INDIGENT ACUTE PSYCHIATRIC INPATIENT HOSPITAL SERVICES AGREEMENTS

#	Acute Psychiatric Inpatient Hospital DBA Name (Corporation Name)	Supervisorial District	Service Area	Type of Hospital	FFS Medi-Cal Hospital	Sole Source Indigent Hospital
11	Emanate Health Inter-Community Hospital (Emanate Health Medical Center) 210 W. San Bernardino Road Covina, CA 91723	5	3	GACH	X	
12	Encino Hospital Medical Center (Prime Healthcare Services - Encino, LLC.) 16237 Ventura Blvd Encino, CA 91436	3	2	GACH	X	
13	Glendale Memorial Hospital and Health Center (Dignity Health) 1420 S. Central Ave Glendale, CA 91204	5	2	GACH	X	
14	Glendora Oaks Behavioral Health Hospital (East Valley Glendora Hospital, LLC) 150 West Route 66 Glendora, CA 91740	5	3	APH	X	
15	Huntington Memorial Hospital (Pasadena Hospital Association LTD.) 100 W. California Blvd Pasadena, CA 91109	5	3	GACH	X	

APH: Acute Psychiatric Hospital ***GACH:*** General Acute Care Hospital

COUNTY OF LOS ANGELES - DEPARTMENT OF MENTAL HEALTH

APPROVAL TO EXTEND THE TERM OF 29 EXISTING FEE-FOR-SERVICE MEDI-CAL ACUTE PSYCHIATRIC INPATIENT HOSPITAL SERVICES AGREEMENTS AND TWO SOLE SOURCE INDIGENT ACUTE PSYCHIATRIC INPATIENT HOSPITAL SERVICES AGREEMENTS

#	Acute Psychiatric Inpatient Hospital DBA Name (Corporation Name)	Supervisorial District	Service Area	Type of Hospital	FFS Medi-Cal Hospital	Sole Source Indigent Hospital
16	Joyce Eisenberg Keefer Medical Center (Grancell Village of the Los Angeles Jewish Home for the Aging) 7150 Tampa Ave Reseda, CA 91335	3	2	APH	X	
17	L.A. Downtown Medical Center (L.A. Downtown Medical Center, LLC) 7500 East Hellman Ave Rosemead, CA 91770	1	3	GACH	X	
18	Mission Community Hospital (Deanco Healthcare, LLC) 14850 Roscoe Blvd. Panorama City, CA 91402	3	2	GACH	X	
19	Northridge Hospital Medical Center (Dignity Health) 18300 Roscoe Blvd Northridge, CA 91328	3	2	GACH	X	
20	Pacifica Hospital of the Valley (Pacifica of the Valley Corporation) 9449 San Fernando Road Sun Valley, CA 91352	3	2	GACH	X	

APH: Acute Psychiatric Hospital ***GACH:*** General Acute Care Hospital

COUNTY OF LOS ANGELES - DEPARTMENT OF MENTAL HEALTH

APPROVAL TO EXTEND THE TERM OF 29 EXISTING FEE-FOR-SERVICE MEDI-CAL ACUTE PSYCHIATRIC INPATIENT HOSPITAL SERVICES AGREEMENTS AND TWO SOLE SOURCE INDIGENT ACUTE PSYCHIATRIC INPATIENT HOSPITAL SERVICES AGREEMENTS

#	Acute Psychiatric Inpatient Hospital DBA Name (Corporation Name)	Supervisorial District	Service Area	Type of Hospital	FFS Medi-Cal Hospital	Sole Source Indigent Hospital
21	Providence Little Company of Mary Medical Center San Pedro (Providence Health System-Southern California) 1300 W. 7th Street San Pedro, CA 90732	4	8	GACH	X	
22	San Gabriel Valley Medical Center (AHMC San Gabriel Valley Medical Center, LP) 438 West Las Tunas Drive San Gabriel, CA 91776	5	3	GACH	X	
23	Sherman Oaks Hospital (Prime Healthcare Services II, LLC) 4929 Van Nuys Blvd. Sherman Oaks, CA 91403	3	2	GACH	X	
24	Southern California Hospital at Culver City (Southern California Healthcare System, Inc.) 3828 Delmas Terrace Culver City, CA 90232	2	5	GACH	X	
25	Southern California Hospital at Van Nuys (Southern California Healthcare System, Inc.) 14433 Emelita Street Van Nuys, CA 90051	3	2	GACH	X	

APH: Acute Psychiatric Hospital ***GACH:*** General Acute Care Hospital

COUNTY OF LOS ANGELES - DEPARTMENT OF MENTAL HEALTH

APPROVAL TO EXTEND THE TERM OF 29 EXISTING FEE-FOR-SERVICE MEDI-CAL ACUTE PSYCHIATRIC INPATIENT HOSPITAL SERVICES AGREEMENTS AND TWO SOLE SOURCE INDIGENT ACUTE PSYCHIATRIC INPATIENT HOSPITAL SERVICES AGREEMENTS

#	Acute Psychiatric Inpatient Hospital DBA Name (Corporation Name)	Supervisorial District	Service Area	Type of Hospital	FFS Medi-Cal Hospital	Sole Source Indigent Hospital
26	St. Francis Medical Center 3630 E. Imperial Hwy Lynwood, CA 90262	2	6	GACH	X	
27	Tarzana Treatment Center, Inc. 18646 Oxnard St. Tarzana, CA 9156	3	2	APH	X	
28	The Regents of the University of California on behalf of the Resnick Neuropsychiatric Hospital at UCLA 750 Westwood Blvd., Los Angeles, CA 90024	3	5	APH	X	
29	USC Verdugo Hills Hospital (USC Verdugo Hills Hospital, LLC) 1812 Verdugo Blvd Glendale, CA 91208	5	2	GACH	X	

APH: Acute Psychiatric Hospital ***GACH:*** General Acute Care Hospital

AGREEMENT NO. MH190xxx

AMENDMENT NO. ___

THIS AMENDMENT is made and entered into this ____ day of January, 2021, by and between the County of Los Angeles (hereafter "County") and Aurora Charter Oak Los Angeles, LLC **or** College Hospital - Cerritos (hereafter "Contractor").

WHEREAS, reference is made to the certain document entitled "Indigent – Acute Psychiatric Intensive Inpatient Hospital Services", dated July 1, 2016, and further identified as Agreement Number MH190xxx, including any amendments thereto, (hereafter collectively "Agreement"); and

WHEREAS, on December 1, 2020, the County Board of Supervisors delegated authority to the Director of Mental Health, or designee, to execute amendments to the Agreement; and

WHEREAS, said Agreement provides that changes may be made in the form of a written amendment which is formally approved and executed by the parties; and

WHEREAS, County and Contractor intend to amend the Agreement to extend the term for six months, beginning January 1, 2021; and

WHEREAS, the Maximum Contract Amount (MCA) for the extension is $_____.

WHEREAS, Contractor warrants that it continues to possess the competence, expertise and personnel necessary to provide services consistent with the requirements of this Agreement and consistent with the professional standard of care for these services.

NOW, THEREFORE, County and Contractor agree that the Agreement shall be amended as follows:

1. This amendment is effective as of January 1, 2021.

2. The Agreement is extended for the six-month period of January 1, 2021 through June 30, 2021.

3. The MCA for the extension is $_____.

4. Paragraph 1 (TERM) sub-paragraph (B) (4), shall be revised as follows:

   "(4) Optional Extension Period: The optional extension period shall commence on January 1, 2021 and shall continue in full force and effect through June 30, 2021, unless earlier terminated or extended."

5. Attachment II of the Agreement, Financial Exhibit A (FINANCIAL PROVISIONS), Paragraph D(4) (Reimbursement for Optional Extension Period) shall be revised as follows:

   "(4). REIMBURSEMENT FOR OPTIONAL EXTENSION PERIOD

   (1) The MCA for the Optional Extension Period of January 1, 2021 through and including June 30, 2021, of this Agreement as described in Paragraph I (TERM) of the Agreement shall not exceed _____DOLLARS ($_____) and shall consist of Funded Programs as shown on the Financial Summary."

6. Financial Summary (Attachment III) – ___ for FY 2020-21, shall be deleted in its entirety, and replaced with Financial Summary (Attachment III) - _____ for FY 2020-21 attached hereto and incorporated herein by reference. All references in Agreement to Financial Summary (Attachment III) – __ for FY 2020-21, shall be

deemed amended to state “Financial Summary (Attachment III) - ____ for FY 2020-21.”

7. Contractor shall provide services in accordance with Contractor’s FY _____ Agreement Package for this Agreement and any addenda thereto approved in writing by the County’s Director of Mental Health or designee.

8. Except as provided in this Amendment, all other terms and conditions of the Agreement shall remain in full force and effect.

/

/

/

/

/

/

/

/

/

/

/

/

/

/

/

/

IN WITNESS WHEREOF, the Board of Supervisors of the County of Los Angeles has caused this Amendment to be subscribed by County's Director of Mental Health, or designee, and Contractor has caused this Amendment to be subscribed on its behalf by its duly authorized officer, on the day, month, and year first above written.

COUNTY OF LOS ANGELES

By _____
JONATHAN E. SHERIN, M.D., Ph.D.
Director of Mental Health

_____
CONTRACTOR

By_____

Name _____

Title _____
(AFFIX CORPORATE SEAL HERE)

APPROVED AS TO FORM:
OFFICE OF THE COUNTY COUNSEL

By: Emily D. Issa
Deputy County Counsel

DEPARTMENT OF MENTAL HEALTH

hope. recovery. wellbeing.

JONATHAN E. SHERIN, M.D., Ph.D.
Director

Gregory C. Polk, M.P.A.
Chief Deputy Director

Curley L. Bonds, M.D.
Chief Medical Officer

Lisa H. Wong, Psy.D.
Senior Deputy Director

October 22, 2020

TO: Supervisor Kathryn Barger, Chair
Supervisor Hilda L. Solis
Supervisor Mark Ridley-Thomas
Supervisor Sheila Kuehl
Supervisor Janice Hahn

FROM: Jonathan E. Sherin, M.D., Ph.D.
Director

SUBJECT: **NOTICE OF INTENT TO EXTEND THE TERM OF TWO EXISTING SOLE SOURCE INDIGENT ACUTE PSYCHIATRIC INPATIENT HOSPITAL SERVICES AGREEMENTS**

In accordance with the Los Angeles County Board of Supervisors' (Board) Policy No. 5.100 (Sole Source Contracts), the Department of Mental Health (DMH) is notifying your Board of our Department's intent to extend the term of two existing sole source Indigent Acute Psychiatric Inpatient Hospital Services (Indigent Hospital) Agreements with Aurora Charter Oak-Los Angeles, LLC (Aurora Charter Oak) and College Hospital-Cerritos (College Hospital).

DMH will request that your Board approve an extension effective January 1, 2021 through June 30, 2021, with an option to extend the term for one additional fiscal year, as necessary.

JUSTIFICATION

The current two sole source Indigent Hospital Agreements with Aurora Charter Oak and College Hospital expire on December 31, 2020. DMH and the State Department of Health Care Services (DHCS) are in the process of finalizing the performance measures for the new acute hospital contracts, which requires collaboration with the DHCS and the contractors.

The sole source Indigent Hospital Agreements with Aurora Charter Oak and College Hospital are located in Service Areas (SAs) 3 and 7, which were identified as strategic SAs in the County's Psychiatric Emergency Services (PES) Relief Plan approved by your Board in July 2005 to address overcrowding at County hospitals.

Board approval of the extension will ensure medically necessary acute psychiatric inpatient hospital services are continuously provided for uninsured clients residing in Los Angeles County while DMH and the State of California – DHCS finalize the performance measures for the new contracts.

NOTIFICATION TIMELINE

Pursuant to Board Policy No. 5.100 (Sole Source Contracts) DMH is required to notify your Board at least six months prior to the expiration of an existing contract when departments do not have delegated authority to execute amendments to extend the term. If requested by your Board office or the Chief Executive Office, DMH will place this item on the Health and Mental Health Services Cluster Agenda. DMH is a little behind in notifying your Board of its intent to extend the term of these contracts, as the performance measures for the new acute hospital contracts are still pending approval.

Unless otherwise instructed by your Board office within four weeks of this notice, DMH will present your Board a letter for approval to extend the term of two existing sole source Indigient Hospital Agreements with Aurora Charter Oak and College Hospital to ensure continuous acute psychiatric inpatient hospital services are provided to uninsured clients residing in Los Angeles County.

If you have any questions or concerns, please contact me at (213) 738-4601, or your staff may contact Stella Krikorian, Division Manager, Contracts Development and Administration Division, at (213) 738-4023.

JES:GCP:ES:SK
SC:atm

c: Executive Office, Board of Supervisors
Chief Executive Office
County Counsel
Curley L. Bonds, M.D.
Gregory C. Polk

SOLE SOURCE CHECKLIST

Department Name: Mental Health

☐ New Sole Source Contract

☑ Existing Sole Source Contract Date Sole Source Contract Approved: 06/14/2016

Check (✓)	JUSTIFICATION FOR SOLE SOURCE CONTRACTS **Identify applicable justification and provide documentation for each checked item.**
✔	➢ Only one bona fide source (monopoly) for the service exists; performance and price competition are not available. A monopoly is an "*Exclusive control of the supply of any service in a given market. If more than one source in a given market exists, a monopoly does not exist* ."
	➢ Compliance with applicable statutory and/or regulatory provisions.
	➢ Compliance with State and/or federal programmatic requirements.
	➢ Services provided by other public or County-related entities.
	➢ Services are needed to address an emergent or related time-sensitive need.
	➢ The service provider(s) is required under the provisions of a grant or regulatory requirement.
	➢ Additional services are needed to complete an ongoing task and it would be prohibitively costly in time and money to seek a new service provider.
	➢ Services are needed during the time period required to complete a solicitation for replacement services; provided services are needed for no more than 12 months from the expiration of an existing contract which has no available option periods.
	➢ Maintenance and support services are needed for an existing solution/system during the time to complete a solicitation for a new replacement solution/ system; provided the services are needed for no more than 24 months from the expiration of an existing maintenance and support contract which has no available option periods.
	➢ Maintenance service agreements exist on equipment which must be serviced by the original equipment manufacturer or an authorized service representative.
	➢ It is more cost-effective to obtain services by exercising an option under an existing contract.
	➢ It is in the best economic interest of the County (e.g., significant costs to replace an existing system or infrastructure, administrative cost savings and excessive learning curve for a new service provider, etc.) In such cases, departments must demonstrate due diligence in qualifying the cost-savings or cost-avoidance associated with the best economic interest of the County.

Chief Executive Office

11/17/20

Date