



LOS ANGELES COUNTY

**DEPARTMENT OF
MENTAL HEALTH**

hope. recovery. wellbeing.

**CHIEF INFORMATION OFFICE BUREAU
PROVIDER ADVOCACY OFFICE - SYSTEMS ACCESS UNIT**

EFT DATA ACCESS REQUEST FORM

Please Print All Information

Request Type

New ☐

Renewal ☐

Delete ☐

Please note: Your account will expire 1 year from account creation or renewal.

Instructions

Legal Entity/DHS/FFS (Organizations with Liaisons): Please complete this form in its entirety and create a New Request in the Systems Access Request (SAR) portal. Please upload this form as part of the New Request.

Fee-for-Service Providers (No liaisons): Please complete this form in its entirety and email it to the DMH Systems Access Unit at SystemsAccessUnit@dmh.lacounty.gov.

Original Signatures Required. Incomplete forms will NOT be processed.

Applicant Information

Print Applicant Name: _____

Last 4 digits of SSN: _____ Day of Birth (MM/DD): ____/____ Logon ID: _____

Legal Entity Provider Name: _____

Legal Entity or Provider Number: _____ Telephone Number: _____

E-mail Address: _____

Requestor's Signature: _____ Date: _____

Requesting: Download Access ☒ Upload Access ☒ Confidential Oath & AUP Attached ☐

Authorization

Authorized CEO/Designee Name (Please Print): _____

By signing this form you hereby grant the above employee access to data provided by the Los Angeles County- Department of Mental Health for your organization. This data may include protected Health and/or claiming information, and is subject to protection as required by HIPAA standards and/or guidelines.

CEO/Designee Signature: _____ Date Completed: _____

Contact Person: _____ Phone Number: (____) _____

Contact E-mail: _____

Notice: Upon user termination, it is the Legal Entity's responsibility to notify CIOB via this form. The danger in not terminating the User ID is the user maintains access to your Legal Entity data and the potential to sabotage or misuse client's data exist.



**COUNTY OF LOS ANGELES
AGREEMENT FOR ACCEPTABLE USE
AND CONFIDENTIALITY OF COUNTY INFORMATION ASSETS
NON-LACDMH WORKFORCE MEMBER**

As a County of Los Angeles (County) Workforce Member, and as outlined in Board of Supervisors Policy [6.101](#) "Use of County Information Assets", I understand and agree:

- That I occupy a position of trust, as such I will use County Information Assets in accordance with countywide and Departmental policies, standards, and procedures including, but not limited to, Board of Supervisors Policy [9.015](#) "County Policy of Equity" (CPOE) and Board of Supervisors Policy [9.040](#) "Investigations Of Possible Criminal Activity Within County Government".
- That I am responsible for the security of information and systems to which I have access or to which I may otherwise obtain access even if such access is inadvertent or unintended. I shall maintain the confidentiality of County Information Assets (as defined in Board of Supervisors Policy [6.100](#) – Information Security Policy).
- That County Information Assets must not be used for:
 - Any unlawful purpose;
 - Any purpose detrimental to the County or its interests;
 - Personal financial gain;
 - In any way that undermines or interferes with access to or use of County Information Asset for official County purposes;
 - In any way that hinders productivity, efficiency, customer service, or interferes with other County Workforce Members performance of his/her official job duties.
- That records, files, databases, and systems contain restricted, confidential or internal use information (i.e. non-public information) as well as Public information. I may access, read or handle Non-public information to the extent required to perform my assigned duties. Although I may have access to Non- public information, I agree to not access such information unless it is necessary for the performance of my assigned duties.
- Not to divulge, publish, share, expose or otherwise make known to unauthorized persons, organization or the public any County Non-public Information. I understand that:
 - I may divulge Non-public Information to authorized County staff and managers as necessary to perform my job duties;
 - I may divulge Non-public Information to others only if specifically authorized to do so by federal, state, or local statute, regulation or court order, and with the knowledge of my supervisor or manager;
 - I may not discuss Non-public Information outside of the workplace or outside of my usual work area;
 - To consult my supervisor or manager on any questions I may have concerning whether particular information may be disclosed.
- To report any actual breach of Information Security or a situation that could potentially result in a breach, misuse or crime relating to County Information Assets whether this is on my part or on the part of another person following proper County and Departmental procedures. I understand that I am expected to assist in

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

protecting evidence of crimes relating to Information Assets and will follow the instructions of, and cooperate, with management and any investigative response team.

- I have no expectation of privacy concerning my activities related to the use of, or access to, County Information Assets, including anything I create, store, send, or receive using County Information Assets. My actions may be monitored, logged, stored, made public, and are subject to investigation, audit and review without notice or consent.
- Not possess a County Information Asset without authorization. Although I may be granted authorization to possess and use a County Information Asset for the performance of my duties, I will never be granted any ownership or property rights to County Information Assets. All Information Assets and Information is the property of the County. I must surrender County Information Assets upon request. Any Information Asset retained without authorization will be considered stolen and prosecuted as such.
- Not intentionally, or through negligence, damage or interfere with the operation of County Information Assets.
- Neither, prevent authorized access, nor enable unauthorized access to County Information Assets.
- To not make computer networks or systems available to others unless I have received specific authorization from the Information Owner.
 - Not share my computer identification codes and other authentication mechanisms (e.g., logon identification (ID), computer access codes, account codes, passwords, ID cards/tokens, biometric logons, and smartcards) with any other person or entity. Nor will I keep or maintain any unsecured record of my password(s) to access County Information Assets, whether on paper, in an electronic file.
 - I am accountable for all activities undertaken through my authentication mechanisms (e.g., logon identification (ID), computer access codes, account codes, passwords, ID cards/tokens, biometric logons, and smartcards).
- Not intentionally introduce any malicious software (e.g., computer virus, spyware, worm, key logger, or malicious code), into any County Information Asset or any non-County Information Systems or networks.
- Not subvert or bypass any security measure or system which has been implemented to control or restrict access to County Information Assets and any restricted work areas and facilities.
 - Disable, modify, or delete computer security software (e.g., antivirus, antispymware, firewall, and/or host intrusion prevention software) on County Information Assets. I shall immediately report any indication that a County Information Asset is compromised by malware following proper County and Departmental procedures.
- Not access, create, or distribute (e.g., via email, Instant Messaging or any other means) any offensive materials (e.g., text or images which are defamatory, sexually explicit, racial, harmful, or insensitive) on County Information Assets, unless authorized to do so as a part of my assigned job duties (e.g., law enforcement). I will report any offensive materials observed or received by me on County Information Assets following proper County and Departmental procedures.
- That the Internet is public and uncensored and contains many sites that may be

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

considered offensive in both text and images. I shall use County Internet services in accordance with countywide and Departmental policies and procedures. I understand that County Internet services may be filtered, however, my use of resources provided on the Internet may expose me to offensive materials. I agree to hold County harmless from and against any and all liability and expense should I be inadvertently exposed to such offensive material.

- That County electronic communications (e.g., email, instant messages, etc.) created, sent, and/or stored using County electronic communications services are the property of the County. I will use proper business etiquette when communicating using County electronic communications services.
- Only use County Information Assets to create, exchange, publish, distribute, or disclose in public forums and social media (e.g., blog postings, bulletin boards, chat rooms, Twitter, Instagram, Facebook, MySpace, and other social media services) any information (e.g., personal information, confidential information, political lobbying, religious promotion, and opinions) in accordance with countywide and Departmental policies, standards, and procedures.
- Not store County Non-public Information on any Internet storage site except in accordance with countywide and Departmental policies, standards, and procedures.
- Not copy or otherwise use any copyrighted or other proprietary County Information Assets (e.g., licensed software, documentation, and data), except as permitted by the applicable license agreement and approved by County Department management. Nor will I use County Information Assets to infringe on copyrighted material.
- That noncompliance may result in disciplinary action (e.g., suspension, discharge, denial of access, and termination of contracts) as well as both civil and criminal penalties and that County may seek all possible legal redress.

I HAVE READ AND UNDERSTAND THE ABOVE AGREEMENT:

Business Associate / Contractor Workforce
Member's Name

Business Associate / Contractor
Workforce Member's Signature

Business Associate / Contractor
Workforce Member's ID Number

Date

Business Associate / Contractor
Manager's Name

Business Associate / Contractor
Manager's Signature

Business Associate / Contractor
Manager's Title

Date



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

**CONFIDENTIALITY OATH
Non-LACDMH Workforce Members**

The intent of this Confidentiality Form is to ensure that all County Departments, 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 (W&I) Code, 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 Section 14100.2, a, b, f, and h, W&I Code, 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>

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



**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

The signed copy of this agreement must be maintained by the LACDMH Sponsor