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

COUNTY OF LOS ANGELES
DEPARTMENT OF MENTAL HEALTH
IBHIS ACCESS REQUEST FORM
NON-LACDMH WORKFORCE MEMBER EDITION

	Last Name:	**First Name:**	**Employee ID:**
Applicant	**Payroll Title:**	**Last 4 digit of SS#:**	**Date of birth:**
	Office Address:	**Clinical / Functional Role:**	
		Email:	**Phone:**
	Organization/Provider Name:	**Program Name:**	**Reporting Unit:**
Approver	**Last Name:**	**First Name:**	**Employee ID:**
	Payroll Title:	**Email:**	**Phone:**
Access Request Type:	**New** ☐ **Role Change** ☐ **Temporary suspension** ☐ **Permanent Termination** ☐		
IBHIS Privilege Requested:		**Effective Date:**	**Expiration Date:**
Validation:	**Policy Acknowledgment** ☐ **Signed Forms** ☐ **Up-to-date HIPAA Training** ☐ **Trained to Use IBHIS** ☐		

By submitting this form, I am verifying that the identified user has received and acknowledged the LAC-DMH Policy 550.04 – Access to Integrated Behavioral Health Information System Using Avatar Electronic Health Record System, signed all agreements attached to this policy, his / her County wide HIPAA awareness trainings are up to date, has been appropriately trained in the use of IBHIS, and will be functioning in a position requiring the identified user roles in IBHIS LIVE production environment which is the level of access to the minimum necessary information needed to perform his / her job functions. I have also verified that this individual has a valid/ unexpired County Identification Badge.

I acknowledge that access to this resource must be renewed annually and will ensure that all required documentations are submitted prior to this request's anniversary date so that the user's access is not impacted. If the action to take is to remove the user's role, then I am verifying that the identified user no longer needs access, or is no longer under my authority, and / or has completed all expected work within the IBHIS LIVE production environment for which I am his/her manager.

Non-DMH Approver's Signature **Print Name** **Date**

FOR LACDMH USE ONLY	
Approved ☐ **Denied** ☐	**Comments:**

LACDMH Sponsor's Signature **Print Name** **Date Received**

LACDMH Local User Administrator's Signature **Print Name** **Date Completed**

Only authorized personnel in association with the Non-DMH Organization shall send the "Access Request to IBHIS" form and required documents.
The packet must be sent to the designated LACDMH Sponsor. Inquiries received from other sources or in other formats including incomplete forms will not be processed.

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

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, antispyware, 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

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

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

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

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

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

I understand that County Departments, 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 the W&I Code (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 provision of the W&I Code 5330 Sections:
    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. 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 W&I Code, 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 office of employment. 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**

Organization 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

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

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

SECURITY AGREEMENT
NON-LACDMH USER

It is the policy of the County of Los Angeles and the Department of Mental Health (LACDMH) that each County employee, whether permanent, temporary, part-time, contract, or in any other status, is individually responsible for the protection of all confidential applicant and participant information, as well as all County information, data, and information processing resources to which he or she has been provided access to.

As a Non-LACDMH workforce member, you may have access to confidential mental health information about clients contained within LACDMH applications, systems, resources and DMH Electronic Health Record Systems. All Non-LACDMH workforce members have an obligation to protect this sensitive information.

As a user of LACDMH System, I understand that my responsibilities include, but are not limited to, the following:

1. All sensitive information obtained from LACDMH systems and resources is confidential and shall not be disclosed to any unauthorized person(s) or group(s). If in doubt, I must consult with my immediate supervisor or manager.

2. I must always protect the privacy and confidentiality of LACDMH clients, and I acknowledge that data browsing is strictly prohibited.

3. I am responsible for the secrecy of my password. My password must neither be written down nor told to anyone. If I know or suspect that my password is known by someone other than myself, I must immediately change my password, and notify the Help Desk, my immediate supervisor or manager.

4. I am not permitted to allow any other person to logon or access DMH systems and resources using my password.

5. I may only use DMH systems and resources for those specific functions for which I am authorized. Personal, non-County business, and/or unauthorized use of LACDMH systems and resources are forbidden.

6. I understand that it is illegal for me to knowingly access LACDMH systems and resources to add, delete, alter, damage, destroy, copy or otherwise use the system to defraud, deceive, extort, or control data for wrongful personal gain.

7. I understand that my access to confidential information in all LACDMH systems and resources is logged and may be audited at any time.

8. I must dispose of documents or other media that are no longer needed using an LACDMH Chief Information Office Bureau (CIOB) approved method that protects confidentiality as documented in LACDMH Policy 554.01, Device and Media Control Policy.

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

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

9. Only data that I believe to be correct may be entered into LACDMH systems and resources. I am not to enter any data which I know or believe to be incorrect. I must notify my immediately supervisor, and if necessary, my chain of command, if I am ever requested to knowingly enter incorrect data.

10. I must Log-off from LACDMH systems and resources or lock and secure my workstation when unattended.

11. I am not permitted to copy, export, download, store, save, print or capture screen displays, photograph or video-graph data from LACDMH systems and resources without prior written authorization from LACDMH Departmental Privacy and Security Officers unless the action listed above is an approved part of conducting business as defined by my role.

12. I am not permitted to install, transmit, copy or download any software from or into LACDMH systems and resources without specific written authorization from LACDMH CIOB management.

13. I am not permitted to connect or disconnect any hardware or peripherals to or from LACDMH systems and resources without specific written LACDMH CIOB management authorization.

14. I must immediately report to my direct supervisor or manager any suspected violation of this LACDMH User Security Agreement, and/or any misuse or non-compliance with any LACDMH systems and resources operating standards and procedures.

I have read and understand this entire User Security Agreement and agree to abide by it. I recognize that my failure to fulfill these responsibilities, including the knowledge of anyone else using my password, could result in the abuse of County information resources and data, and that the County may hold me responsible for such abuse.

I further understand that any violation of this agreement may result in disciplinary action up to and including discharge. I also have been informed that failure to comply with Health Insurance Portability and Accountability Act of 1996 (HIPAA) can result in civil and criminal penalties per 42 USC § 1320d-5.

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

Business Associate / Contractor Approver: As a representative and liaison of the Non-LACDMH organization 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 Security 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